USER'S GUIDE
network management card

Contents

Introduction 1

Product Description 1
Features 1
Initial set-up 2
Network management features 3

Internal Management Features 4
Overview 4
Login control 4
Types of user accounts 5

Front Panel 6
Introduction 6
Features 8
Status LED 9
Link-RX/TX (10/100) LED 10

Watchdog Features 11
Overview 11
Network interface watchdog mechanism 11
Resetting the network timer 12

Control Console 13

How To Log On 13
Overview 13
Remote access to the control console 13
Local access to the control console 14

How to Recover from a Lost Password 15

Main Screen 16
Example main screen 16
Information and status fields 17

Control Console Menus 19
Overview 19
Main menu 19
Menu structure 20
Device Manager option 21
Network option 21
System option 22

Web Interface 23

Introduction 23
Overview 23
Supported Web browsers 24
How to Log On 25
Overview 25
URL address formats 26
Summary Page 27
Example Web page 27
"Summary" page fields 28
Quick status tab 29
Navigation Menu 31
Overview 31
Selecting a menu to perform a task 32
Help menu 33
Links menu 34

Network Menu 35

Introduction 35
Overview 35
Menu options 36

Option Settings 37
TCP/IP 37
DNS 40
Ping utility (control console) 41
FTP Server 41
Telnet/SSH 42
SNMP 49
Email 50
Syslog 51
Web/SSL/TLS 54

System Menu 61

Introduction 61
Overview 61
Menu options 62

Option Settings 63
User Manager 63
Identification 65
Date & Time 66
Tools 67
Preferences (Web interface) 68
Links (Web interface) 68
Modem (AP9618 control console) 69
About System 70

UPS Menu 71

Introduction 71
Overview 71
UPS menu options 71

UPS Status 72
Overview 72
Detailed UPS Status 73
Utility Power Status 74
Output Power Status 75
Fault Tolerance (Symmetra or Symmetra PX UPS) 77
Battery Status 78

Diagnostics 79
Overview 79
Diagnostic tests 79
Scheduled UPS self-tests 81
Control 82
Initiating a UPS Control option 82
Configuration 89
Overview 89
Utility Line Settings 90
Alarm Thresholds (Symmetra UPS or Symmetra PX UPS) 91
Shutdown Parameters 92
General Settings 94
Reset UPS Defaults 95
Configure Parallel UPS parameters (Silcon UPS only) 95
Module Status (Symmetra UPS or Symmetra PX UPS) 96
Menu options 96
Module status 96
PowerChute (UPS PowerChute Network Shutdown) 97
Overview 97
PowerChute Network Shutdown Parameters 98
Maximum-Shutdown-Time negotiation 99
Scheduling (UPS Shutdown) 101
Overview 101
Examples 102
How to schedule a shutdown 103
How to schedule a synchronized shutdown 104
How to edit, disable, or delete a shutdown 105
Sync Control 106
Overview 106
Sync Control Group Status 106
Configure Synchronized Control 107

Environment Menu 109

Introduction 109
Overview 109
Environment menu options 109
Status Options 110
Overview 110
Probe status 111
Contact status 111
Output relay status (AP9618 or AP9619) 111
Settings Options. 112
Probe settings 112
Contact settings 112
Output relay settings (AP9618 or AP9619) 113

Event-Related Menus 114

Introduction 114
Overview 114
Menu options 115
Event Log 116
Overview 116
Logged events 117
Web interface 117
Control console 118
How to use FTP or SCP to retrieve log files 118
Event Actions (Web Interface Only) 121
Overview 121
Severity levels 122
Event Log action 122
Syslog action 123
SNMP Traps action 123
Email action 123
Event Recipients. 124
Overview 124
Trap Receivers 125
Email options 125

E-mail Feature 126
Overview 126
DNS servers 127
SMTP settings 127
Email Recipients 128
How to Configure Individual Events 131
"Event List" page 131
"Detailed Event Action Configuration" page 131

Data Menu (Web Interface Only) 132

Log Option 132
Configuration Option 133

Boot Mode 134

Introduction 134
Overview 134
DHCP & BOOTP boot process 135
DHCP Configuration Settings 137
Management Card settings 137
DHCP response options 139

Security 143

Security Features 143
Planning and implementing security features 143
Summary of access methods 143
Changing default user names and passwords immediately 145
Port assignments 145
User names, passwords, community names (SNMP) 146
Authentication 147
Authentication versus encryption 147
MD5 authentication (for the Web interface) 148
Encryption 150
Secure SHell (SSH) and Secure CoPy (SCP) 150
Secure Socket Layer (SSL)/Transport Layer Security (TLS) 152

Creating and Installing Digital Certificates 154
Purpose 154
Choosing a method for your system 155
Firewalls 161

Troubleshooting 162

Management Card 162
Management Card access problems 162
SNMP issues 164
Synchronization problems 164

Product Information 165

Warranty and Service 165
Limited warranty 165
Warranty limitations 166
Obtaining service 167
Recycling the Battery 167
Life-Support Policy 168
General policy 168
Examples of life-support devices 168
Specifications 169
Electrical 169
Physical 169

Index 170

Introduction

Product Description

Features

The following APC Network Management Cards are web-based management products that use multiple, open standards such as Telnet, HTTP, HTTPS, SSL, TLS, SCP, and SNMP to provide full management of supported devices:

- AP9617 Network Management Card *EX*: The following is a list of some of this Management Card's features:
  - Generates system log (Syslog) messages
  - Allows using a Dynamic Host Configuration Protocol (DHCP) server to provide the Management Card's network (TCP/IP) values
  - Allows using the APC Remote Monitoring Service (RMS)
  - Provides data and event Logs
  - Provides UPS scheduling features
  - Provides support for the APC PowerChute® Network Shutdown utility
  - Limits SNMP traps and e-mail notifications based on the severity level of the UPS or system events
  - Provides a selection of security protocols for authentication and encryption.
- AP9618 Network Management Card *EM/MDM*: Includes all AP9617 features, an Integrated Environmental Monitor that includes an output relay, and an internal analog modem.
- AP9619 Network Management Card *EM*: Includes all AP9617 features

and an Integrated Environmental Monitor that includes an output relay.

Kits are available to upgrade AP9617 to include the features of AP9618 (AP9618U kit) or AP9619 (AP9619U kit). The AP9618U kit can also upgrade an AP9619 Management Card to include the AP9618 analog modem feature.

The Management Card can be installed into the following APC devices:

- Any Smart-UPS® or Matrix-UPS® model that has an internal expansion slot, as well as any Silcon™, Symmetra®, or Symmetra PX UPS

A Silcon UPS, which does not have an expansion slot, requires using a Silcon Triple Expansion Chassis (AP9604S).

- Expansion Chassis (AP9600)
- Triple Expansion Chassis (AP9604)

Initial set-up

You must define three TCP/IP settings for the Network Management Card before it can operate on the network.

- IP address of the Management Card
- Subnet mask
- IP address of the default gateway

To configure the TCP/IP settings, see the Network Management Card *Installation and Quick Start Manual* provided in PDF (**.\doc\Insguide.pdf**) on the APC Network Management Card *utility* CD and in printed form.

To use a DHCP server to configure the TCP/IP settings at a Management Card, see Boot Mode.

Network management features

Following are some of the network management applications and utilities that can work with a UPS that connects to the network through a Network Management Card.

- APC network management applications:
  - PowerChute Network Shutdown provides unattended graceful shutdown of computers that are connected serially to the UPS.
  - APC Enterprise Manager provides enterprise-level power management and diagnostics for APC UPS systems.
  - PowerChute Business Edition provides departmental-level safe system shutdown and UPS management for workstations and servers.
  - APC InfraStruXure™ Manager provides the power management software for an InfraStruXure system.
- APC Wizard utilities
  - The APC Management Card Wizard configures multiple Network Management Cards over the network. (You cannot use it to download firmware upgrades to the Network Management Card.)
  - The APC Security Wizard creates components needed for high security for the Network Management Card on the network when you are using Secure Socket Layer (SSL) and related protocols and encryption routines.
- APC Enterprise Manager provides enterprise-level power management and device management for APC agents, UPS models, information controllers, and environmental monitors
- A Management Information Base (MIB) browser uses the OIDs of the APC PowerNet MIB to perform SNMP SETs and GETs on a UPS.

Internal Management Features

Overview

The Management Card has two internal interfaces (control console and Web interface) which provide menus with options that allow you to manage the UPS, an environmental monitor (including the Integrated Environmental Monitor at an AP9618 or AP9619 Network Management Card), and the Management Card. The Management Card's SNMP interface also allows you to use an SNMP browser with the PowerNet MIB to manage the UPS and environmental monitor.

For more information about the Management Card's internal user interfaces, see Control Console and Web Interface; for more information about how to use the PowerNet MIB with an SNMP browser, see the *PowerNet® SNMP Management Information Base (MIB) Reference Guide* (**.\doc\Mibguide.pdf**), which is provided on the APC Network Management Card *utility* CD.

Login control

Only one user at a time can log on to the Management Card to use its internal user interface features. The priority for access is as follows:

- Local access to the control console from a computer with a direct serial connection to the Management Card always has the highest priority
- Telnet or Secure SHell (SSH) access to the control console from a remote computer has the next highest priority
- Web access has the lowest priority

For information about how SNMP access to the Management Card is controlled, see SNMP.

Types of user accounts

The Management Card has three levels of access (Administrator, Device Manager, and Read-only User), all of which are protected by user name and password requirements.

- An Administrator can use all of the management menus available in the control console and the Web interface. The Administrator's default **User Name** and **Password** are both **apc**.
- A Device Manager can access only the **Log** option in the **Events** menu and use the UPS and **Environment** menus. The Device Manager's default user name is **device**, and the default password is **apc**.
- A Read-Only User has the following restricted access:
  - Access through the Web interface only.
  - Access to the same menus as a Device Manager, but without the capability to change configurations, control devices, or delete data. Links to configuration options are visible but are disabled, and the event and data logs display no **Delete** button.

  The Read-Only User's default **User Name** is **readonly**, and the default **Password** is **apc**.

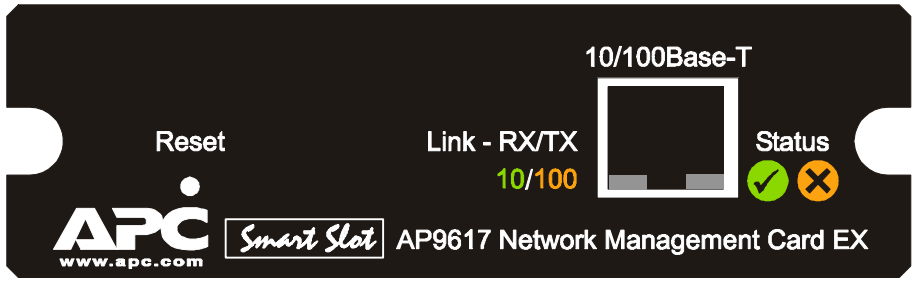
To set **User Name** and **Password** values for the three account types, see User Manager.

You must use the Web interface to configure values for the Read-Only User.

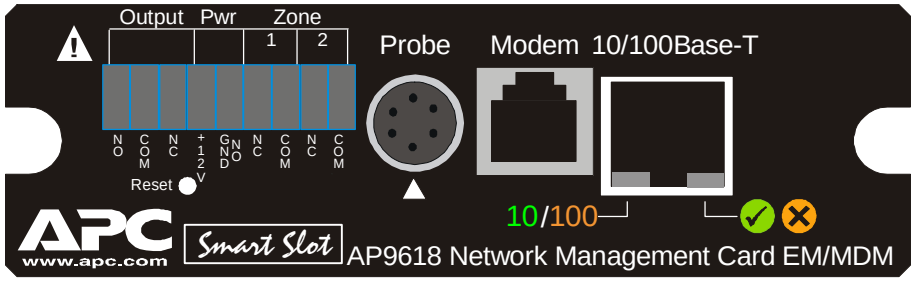
Front Panel

Introduction

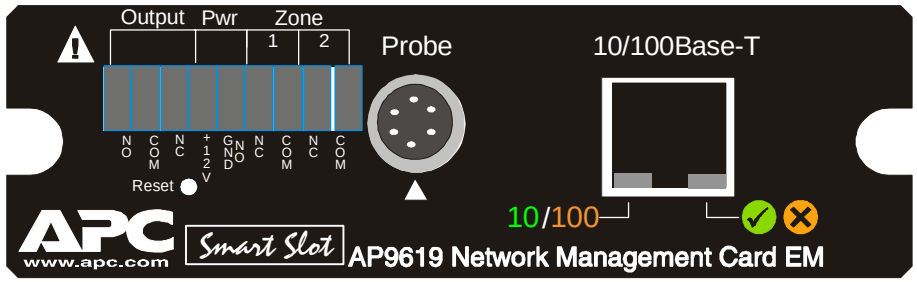
The figures below identify the front-panel features of the three versions (AP9617, AP9618, and AP9619) of the Network Management Card.



Includes Status LEDs, Reset button, and 10/100Base-T connector.



Includes the AP9617 features, an analog modem connector, and the Integrated Environmental Monitor's connections (probe, input contacts, and output relay contacts).



Includes AP9617 features and the Integrated Environmental Monitor's connections (probe, input contacts, and output relay contacts).

Features

AP9618 or AP9619	Description
9-pin connector[1]	• Output relay (**Output**): Normally closed (**NC**), common (**COM**), and normally open (**NO**) pins used by the Integrated Environmental Monitor's output relay at an AP9618 or AP9619 Management Card. • Power (**Pwr**): Normally-open ground (**GND NO**) and **+12VDC** pins. • Input contacts (**Zone 1** and **2**): Two sets of normally closed (**NC**) and common (**COM**) pins used by the Integrated Environmental Monitor at an AP9618 or AP9619 Management Card.
Probe connector[1]	Connects a Temperature/Humidity probe to the Integrated Environmental Monitor at the AP9618 or AP9619 Management Card.
Modem connector[2] (AP9618 only)	Connects the internal analog modem at an AP9618 Management Card to an analog phone line to provide for out-of-band communications.
All Management Cards	**Description**
Reset button	Resets the Management Card while power remains on.
10/100 Base-T connector	Connects the Management Card to the Ethernet network.
Status LEDs	See Status LED.
Link-RX/TX (10/100) LED	See Link-RX/TX (10/100) LED.

1 To manage the Integrated Environmental Monitor, see Environment Menu.
2 To configure this feature for dial-in access to the control console at an AP9618 Network Management Card, see Modem (AP9618 control console).

Status LED

This LED indicate the Management Card's status.

Condition	Description
Off	One of the following situations exist: • The Management Card is not receiving input power • The Management Card is starting up. • The Management Card is not operating properly. It may need to be repaired or replaced. Contact APC Worldwide Customer Support.
Solid **Green**	The Management Card has valid TCP/IP settings.
Solid **Orange**	A hardware failure has been detected in the Management Card. Contact APC Worldwide Customer Support.
Flashing **Green**	The Management Card does not have valid TCP/IP settings.[1]
Flashing **Orange**	The Management Card is making BOOTP[2] requests.[1]
Alternately flashing **Green** and **Orange**	The Management Card is making DHCP[3] requests.[1]

1 If you do not use a BOOTP or DHCP server, see the Network Management Card *Installation and Quick Start Manual* provided in printed format, and in PDF (**.\doc\Insguide.pdf**) on the APC Network Management Card *utility* CD to configure the Management Card's TCP/IP settings.
2 To use a BOOTP server, see the Management Card *Addendum* (**.\doc\Addendum.pdf**) on the APC Network Management Card *utility* CD.
3 To use a DHCP server, see Boot Mode.

Link-RX/TX (10/100) LED

This LED indicates the network status.

Condition	Description
Off	One or more of the following situations exist: • The Management Card is not receiving input power. • The cable that connects the Management Card to the network is disconnected or defective. • The device that connects the Management Card to the network is turned off or not operating correctly. • The Management Card itself is not operating properly. It may need to be repaired or replaced. Contact APC Worldwide Customer Support.
Solid **Green**	The Management Card is connected to a network operating at 10 Megabits per second (Mbps).
Solid **Orange**	The Management Card is connected to a network operating at 100 Megabits per second (Mbps).
Flashing **Green**	The Management Card is receiving or transmitting data packets at 10 Megabits per second (Mbps).
Flashing **Orange**	The Management Card is receiving or transmitting data packets at 100 Megabits per second (Mbps).

Note

Using the 5-Port 10Base-T Hub SmartSlot Card eliminates the requirement for a separate hub power supply. However, this card requires that all Network Management Cards connected to it operate at 10 Mbps, not 100 Mbps.

Watchdog Features

Overview

To detect internal problems and recover from unanticipated inputs, the Management Card uses internal, system-wide watchdog mechanisms. When it restarts to recover from an internal problem, a **System: Warmstart** event is recorded in the Event Log.

Network interface watchdog mechanism

The Management Card implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the Management Card does not receive any network traffic for 9.5 minutes (either direct traffic, such as SNMP, or broadcast traffic, such as an Address Resolution Protocol [ARP] request), it assumes that there is a problem with its network interface and restarts.

Resetting the network timer

To ensure that the Management Card does not restart if the network is quiet for 9.5 minutes, the Management Card attempts to contact the Default Gateway every 4.5 minutes. If the gateway is present, it responds to the Management Card, and that response restarts the 9.5-minute timer. If your application does not require or have a gateway, specify the IP address of a computer that is running on the network most of the time and is on the same subnet. The network traffic of that computer will restart the 9.5-minute timer frequently enough to prevent the Management Card from restarting.

Control Console

How To Log On

Overview

You can use either a local (serial) connection, or a remote (Telnet) connection with a computer on the Management Card's subnet to access the control console. For an AP9618 Network Management Card, you can also use its internal analog modem to access the control console (see Modem (AP9618 control console)).

Use case-sensitive **User Name** and **Password** entries to log on (by default, **apc** and **apc**, for an Administrator, or **device** and **apc**, for a Device Manager). A Read Only User has no access to the control console.

If you cannot remember your **User Name** or **Password**, see How to Recover from a Lost Password.

Remote access to the control console

You can use Telnet to log on to the control console from any computer on the same subnet as the Management Card.

1. At a command prompt, type `telnet` and the Management Card's System IP address, and then press ENTER. For example:
   `telnet 139.225.6.133`
2. Enter your **User Name** and **Password**.

Local access to the control console

You can use a local computer, a computer that connects to the Management Card through the serial port at the Management Card's UPS or expansion chassis, to access the control console.

1. Select a serial port at the local computer and disable any service which uses that port.
2. Unless an APC smart-signaling cable (940-0024 or 940-1524) is already connected to the selected port, connect the smart-signaling cable that came with the Management Card to the selected port and to the serial port at the Management Card's UPS or chassis.
3. Run a terminal program (such as HyperTerminal) and configure the selected port for 2400 bps, 8 data bits, no parity, 1 stop bit, and no flow control, and save the changes.
4. Press ENTER to display the **User Name** prompt.
5. Enter your **User Name** and **Password**.

How to Recover from a Lost Password

You can use a local computer, a computer that connects to the Management Card through the serial port at the Management Card's UPS or expansion chassis, to access the control console.

1. Select a serial port at the local computer and disable any service which uses that port.
2. Unless an APC smart-signaling cable (940-0024 or 940-1524) is already connected to the selected port, connect the smart-signaling cable that came with the Management Card to the selected port and to the serial port at the Management Card's UPS or chassis.
3. Run a terminal program (such as HyperTerminal) and configure the selected port for 2400 bps, 8 data bits, no parity, 1 stop bit, and no flow control, and save the changes.
4. Press ENTER to display the **User Name** prompt.
5. Press the Reset button on the Network Management Card, which causes the it to restart, a process that takes approximately 15 seconds.
6. Press ENTER as many times as necessary to redisplay the **User Name** prompt, then use **apc** for the user name and password. (If you take longer than 30 seconds to log on after the **User Name** prompt is redisplayed, you must start the login procedure again at step 4.)
7. From the **Control Console** menu, select **System**, then **User Manager**.
8. Select **Administrator**, and change the **User Name** and **Password** settings, both of which are now defined as **apc**.
9. Press CTRL-C and log off.

Reconnect any cable disconnected in step 2, and restart any service disabled in step 1.

Main Screen

Example main screen

The following is an example of the screen that appears when you log on to the control console at an AP9618 or AP9619 Management Card that has the Integrated Environmental Monitor's output relay enabled (an AP9617 does not have an Integrated Environmental Monitor, so it cannot report status for an output relay).

Note

The **Relay OK** entry in the **Environment** status line indicates that the output relay is enabled and that no alarm condition exists.

```
American Power Conversion               Network Management Card AOS     v2.1.0
<c> Copyright 2003 All Rights Reserved  Smart-UPS & Matrix-UPS APP      v2.1.0
-------------------------------------------------------------------------------
Name      : Test Lab                                  Date : 06/10/2003
Contact   : Don Adams                                 Time : 05:58:30
Location  : Building 3                                User : Administrator
Up Time   : 0 Days, 21 Hours, 21 Minutes              Stat : P+ N+ A+

Thresholds OK, Contact Alarms OK, Relays OK
Smart-UPS 700 named Tester 8  : On Line

------- Control Console -----------------------------------------------------

     1- Device Manager
     2- Network
     3- System
     4- Logout

     <ESC>- Main Menu, <ENTER>- Refresh, <CTRL-L>- Event Log
>
```

Information and status fields

Main screen information fields.

- Two fields identify the APC operating system (AOS) and application (APP) firmware versions. The application firmware uses a name that identifies the type of UPS that the Management Card connects to the network. In the preceding example, the Management Card uses the application firmware for a UPS in the Smart-UPS/Matrix-UPS family, in this case, the Smart-UPS 700.

```
Network Management Card AOS   v2.0.1
Smart UPS & Matrix UPS APP    v2.0.1
```

- Three fields identify the system **Name**, **Contact**, and **Location** values.

```
Name      : Test Lab
Contact   : Don Adams
Location  : Building 3
```

For information about how to set the **Name**, **Contact**, and **Location** values, see System Menu.

- An **Up Time** field reports how long the Management Card has been running since it was last turned on or reset.

```
Up Time   : 0 Days 21 Hours 21 Minutes
```

- Two fields identify when you logged in, by **Date** and **Time**.

```
Date : 03/23/2003
Time : 5:58:20
```

- A **User** field identifies whether you logged in as **Administrator** or **Device Manager**. (The **Read Only User** account cannot access the Control Console.)

```
User : Administrator
```

Main screen status fields.

- A **Stat** field reports the Management Card status.

```
Stat : P+ N+ A+
```

P+	The APC operating system (AOS) is functioning properly.
N+	The network is functioning properly.
N?	A BOOTP request cycle is in progress.
N–	The Management Card failed to connect to the network.
N!	Another device is using the Management Card's IP address.
A+	The application is functioning properly.
A–	The application has a bad checksum.
A?	The application is initializing.
A!	The application is not compatible with the AOS.

The AOS should always report that it is functioning properly (P+); If the AOS is not functioning properly, and you can not access the Management Card, see APC Worldwide Customer Support to contact APC support staff.

- A **UPS model and name** field reports the status of the UPS.

```
Smart-UPS 700 RM named Tester 8 : On Line
```

- The status of the probes (**Thresholds**) and contacts (**Contact Alarms**) at any environmental monitor, including the Integrated Environmental Monitor's output relay (**Relay**) at an AP9618 or AP9619 Management Card, is reported above the UPS status (**UPS model and name**) field.

```
Thresholds Ok, Contact Alarms Ok, Relay OK
```

For more information about the UPS status, see UPS Status; for more information about probe, contact, and output relay status, see Environment Menu.

Control Console Menus

Overview

The control console dynamically expands to provide options that you use to manage a Management Card, its UPS, and other supported devices. If a device is not present, the control console displays no options for that device. For example:

- The control console at a Management Card that connects with an environmental monitor only, does not provide UPS options.
- The control console at an AP9618 or AP9619 Network Management Card displays options that you use to manage the Management Card's Integrated Environmental Monitor. These options are not available at the control console for an AP9617.

Main menu

The main **Control Console** menu has options that provide access to the control console's management features:

```
1- Device Manager
2- Network
3- System
4- Logout
```

When you log on as Device Manager, you can access only the **Device Manager** menus and the **Logout** menu.

Menu structure

The menus in the control console list options by number and name. To use an option, type the option's number and press ENTER, then follow any on-screen instructions.

Some options access a new menu; other options allow you to change a setting. Menus that allow you to change a setting have an **Accept Changes** option which you must use before you exit a menu to save the changes you made.

While in a menu, you can also do the following:

- Type ? and press ENTER, to access brief menu option descriptions (if the menu has help available)
- Press ENTER, to refresh the menu
- Press ESC, to go back to the menu from which you accessed the current menu
- Press CTRL-C, to return to the main (**Control Console**) menu
- Press CTRL-D, to toggle between the UPS and **Environment** menus
- Press CTRL-L, to access the event log

For information about the event log, see Event-Related Menus.

Device Manager option

This option accesses the **Device Manager** menu. This menu's options allow you to select the device that you want to manage:

```
1- Smart-UPS 700
2- Environment
```

The Environment option is present only when an environmental monitor is present. For an AP9618 or AP9619 Network Management Card, the Environment option accesses the menu options you use to configure the Integrated Environmental Monitor, as well as an external environmental monitor.

For information about the menu options that are available for managing a UPS, see UPS Menu; for information about the menu options that are available for managing environmental monitors, including the Integrated Environmental Monitor at an AP9618 or AP9619 Network Management Card, see Environment Menu.

Network option

To do any of the following tasks, see Network Menu:

- Configure the Management Card's TCP/IP settings, or, when the Management Card will obtain its TCP/IP settings from a server, configure the settings for the type of server (DHCP or BOOTP) to be used.
- Use the Ping utility.
- Define settings that affect the Management Card's FTP, Telnet, Web interface, SNMP, E-mail, DNS, and Syslog features.

System option

To do any of the following tasks, see System Menu:

- Control **Administrator** and **Device Manager** access. (You can control **Read Only User** access by using only the Web interface.)
- Define the system **Name**, **Contact**, and **Location** values.
- Set the **Date** and **Time** used by the Management Card.
- Restart the Management Card.
- Reset control console settings to their default values.
- Configure dial-in access to the control console at an AP9618 Network Management Card using the Management Card's internal analog modem.
- Access system information about the Management Card.

Web Interface

Introduction

Overview

The Web interface provides options that you use to manage a Management Card, its UPS, and other supported devices (if a device is not present, the Web interface displays no options for that device). For example:

- The Web interface at a Management Card that connects with an environmental monitor only, will not provide UPS options.
- The Web interface at an AP9618 or AP9619 Network Management Card displays options that you use to manage the Management Card's Integrated Environmental Monitor. These options would not be available at the Web interface for an AP9617 Management Card, which has no Integrated Environmental Monitor.

See Web/SSL/TLS for information on the menu options you use to select, enable, and disable the protocols that control access to the Web interface and to define the Web-server ports for the protocols.

Supported Web browsers

As your browser, you can use Microsoft® Internet Explorer (IE) 5.0 (and higher) or Netscape® 4.0.8 (and higher, except Netscape 6.*x*) to access the Management Card through its Web interface. Other commonly available browsers also may work but have not been fully tested by APC.

Data verification, the event log, the data log, and Message Digest 5 (MD5) authentication require that you enable the following for your Web browser:

- JavaScript
- Java
- Cookies

In addition, the Management Card cannot work with a proxy server. Therefore, before you can use a Web browser to access its Web interface, you must do one of the following:

- Configure the Web browser to disable the use of a proxy server for the Management Card.
- Configure the proxy server so that it does not proxy the specific IP address of the Management Card.

How to Log On

Overview

You can use a Management Card's DNS name or System IP address for the URL address of the Web interface. Use your case-sensitive **User Name** and **Password** settings to log on. The default user name differs by account type:

- **apc** for an Administrator
- **device** for a Device Manager
- **readonly** for a Read Only User

The default password is **apc** for all three account types.

If you are using HTTPS (SSL/TSL) as your access protocol, your login credentials are compared with information in a server certificate. If the certificate was created with the APC Security Wizard, you must use an IP address to log on to the Management Card if an IP address was specified as the common name in the certificate, or you must use a DNS name to log on if a DNS name was specified as the common name in the certificate.

For information about the Web page that appears when you log on to the Web interface, see Summary Page.

URL address formats

Type the Management Card's DNS name or IP address in the Web browser's URL address field and press ENTER. Except when you specify a non-default web server port in Internet Explorer, `http://` or `https://` is automatically added by the browser.

If the error "You are not authorized to view this page" occurs (Internet Explorer only), someone is logged onto the Web interface or control console. If the error "No Response" (Netscape) or "This page cannot be displayed" (Internet Explorer) occurs, Web access may be disabled, or the Management Card may use a non-default Web-server port that you did not specify correctly in the address.

- For a DNS name of Web1, the entry would be one of the following:
  - `http://Web1` if HTTP is your access mode
  - `https://Web1` if HTTPS (SSL/TLS) is your access mode
- For a System IP address of 139.225.6.133, when the Management Card uses the default port (80) at the Web server, the entry would be one of the following:
  - `http://139.225.6.133` if HTTP is your access mode
  - `https//139.225.6.133` if HTTPS (SSL/TLS) is your access mode
- For a System IP address of 139.225.6.133, when the Management Card uses a non-default port (5000, in this example) at the Web server, the entry would be one of the following:
  - `http://139.225.6.133:5000` if HTTP is your access mode
  - `https://139.225.6.133:5000` if HTTPS (SSL/TLS is your access mode

Summary Page

Example Web page

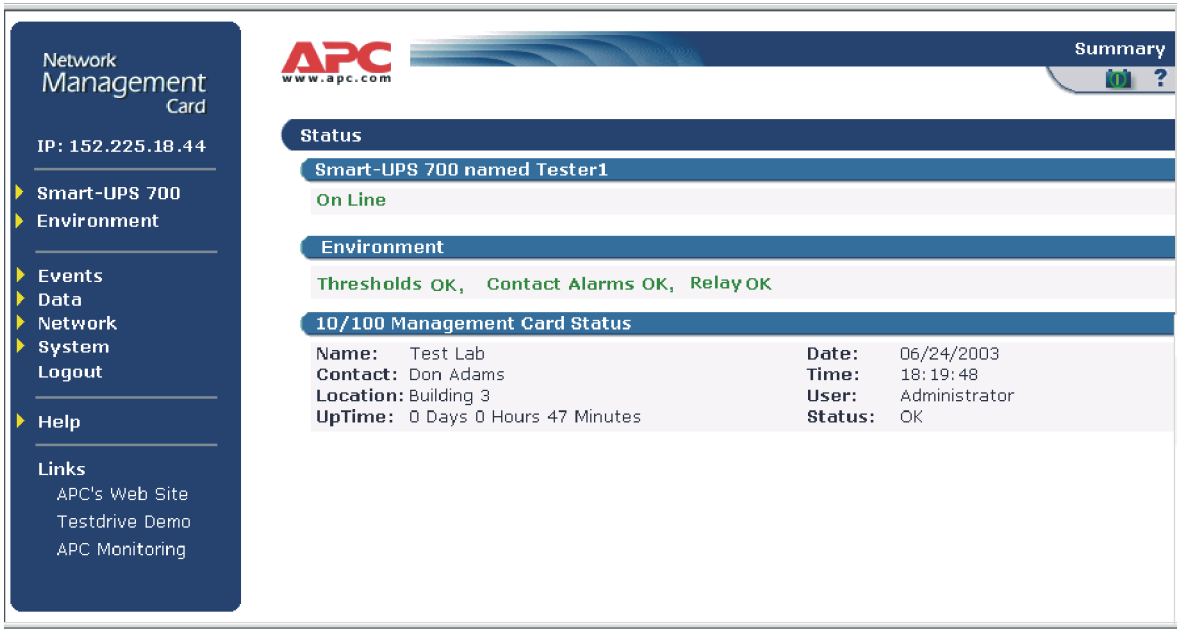
A navigation menu (see Navigation Menu) and "Summary" page are displayed when you log on to the Web interface at an AP9618 or AP9619 Management Card that has the Integrated Environmental Monitor's output relay enabled. (An AP9617 has no output relay.)

Note

The **Relay OK** entry in the **Environment** status line indicates that the output relay is enabled and that no alarm condition exists.

After the Management Card connects with a UPS, you can click the battery status icon on any Web interface page to access the "Summary Page."

For more information about the help and status icons that can appear in the Web interface pages, see Quick status tab.



"Summary" page fields

The "Summary" page has three sections:

- The UPS section reports the status of a connected UPS.
- The **Environment** section reports status information for any connected environmental monitor, including the Integrated Environmental Monitor's output relay at an AP9618 or AP9619 Network Management Card.
- The **Management Card** section reports the following information:
  - The **Name**, **Contact**, and **Location** information for the Management Card
  - The login date and time
  - Type of user (**Administrator**, **Device Manager**, or **Read Only User**)
  - How long (**Up Time**) the Management Card has been continuously running since it was turned on or reset
  - The status of the Management Card

Quick status tab

Three types of icons can appear in the quick status tab in the upper-right corner of every Web interface page:

- A question mark (?) provides access to the online help for that page:

- When a UPS is connected, a battery icon identifies the current status of the UPS and accesses the “Summary” page from any other page:

The UPS is switched to bypass mode.

The UPS is operating normally.

The UPS is turned off.

The UPS is overloaded.

The UPS has a bad battery.

The UPS is switched to battery operation.

A fault exists at the UPS.

Communication with the UPS has been lost, or the UPS is unsupported.

- When an environmental monitor is connected, including the Integrated Environmental Monitor at an AP9618 or AP9619, icons will identify any fault conditions:

A high-temperature threshold violation exists.

A low-temperature threshold violation exists.

A high-humidity threshold violation exists.

A low-humidity threshold violation exists.

States which contact device has a fault: either an input contact or the output relay at an AP9618 or AP9619 Management Card's Integrated Environmental Monitor.

Navigation Menu

Overview

When you log on to the Web interface as an Administrator, the navigation menu (left frame) includes the following elements:

- The Management Card's IP address
- A UPS menu which uses the UPS model for its name (**Smart-UPS 700**, in the example on Example Web page)
- An **Environment** menu (if an environmental monitor is used)
- An **Events** menu
- A **Data** menu
- A **Network** menu
- A **System** menu

When you log on as a Device Manager or Read Only User, the **Network** and **System** menus do not appear in the navigation menu. Options to make any changes are not available for the Read Only User.

- A **Logout** option
- A **Help** menu
- A **Links** menu

Selecting a menu to perform a task

Use the menus to perform tasks as follows:

- To manage a UPS, and to set up and manage Synchronized Control Groups of Smart-UPS or Symmetra UPSs, see UPS Menu.
- To manage an environmental monitor, including the AP9618 or AP9619 Network Management Card's Integrated Environmental Monitor, see Environment Menu.
- To do the following, see Event-Related Menus:
  - Access the Event Log.
  - Configure the actions to be taken based on an event's severity level.
  - Configure SNMP Trap Receiver settings to send event-based traps.
  - Define who will receive e-mail notifications of events.
- To do the following, see Data Menu (Web Interface Only):
  - Access the Data Log.
  - Define the log interval (how often data will be sampled and recorded) for the Data Log.
- To do the following, see Network Menu:
  - Configure new TCP/IP settings for the Management Card.
  - Identify the Domain Name Service (DNS) Server, and test the network connection to that server.
  - Define settings for FTP, Telnet, SSH, the Web interface, SNMP, e-mail, and SSL/TLS.
  - Configure the Management Card's Syslog message feature.

- To do the following, see System Menu.
  - Control **Administrator**, **Device Manager**, and **Read Only User** access.
  - Define the system **Name**, **Contact**, and **Location** values.
  - Set the **Date** and **Time** values used by the Management Card.
  - Restart the Management Card.
  - Reset control console settings to default settings.
  - Select **Fahrenheit** or **Celsius** for temperature displays.
  - Define the URL addresses used by the Web interface's user and APC logo links, as described in Links menu.

Help menu

When you click **Help**, the **Contents** for the online help is displayed automatically to provide for easy navigation to a specific online help topic. However, from any of the Web interface pages, you can use the question mark (**?**) that appears in the quick status bar to link to the section of the online help that covers that page's content.

Use the **Help** menu's **About System** option to view information about the Management Card's **Model Number**, **Serial Number**, **Hardware Revision**, **Manufacture Date**, **MAC Address, Application Module** and **APC OS (AOS) Module**, including the date and time these modules were loaded.

In the control console, the **About System** option, which is a **System** menu option, identifies the **Flash Type** used.

Links menu

This menu provides three user-definable URL link options. By default, these links access the following APC web pages:

- **APC's Web Site** accesses the APC home page
- **Testdrive Demo** accesses a demonstration page where you can use samples of APC web-enabled products
- **APC Monitoring** accesses the "APC Remote Monitoring Service" page where you can find more information about monitoring services available from APC at an additional cost.

You can use the following procedure to redefine these links so that they point to other URLs, such as those of other UPS devices, or of the MasterSwitch devices and servers that are being powered by the UPS.

1. Click on **Links** in the **System** menu.
2. Define the any new names for the **User Links**.
3. Define the any new URL addresses that you want the **User Links** to access.
4. Click **Apply**.

Network Menu

Introduction

Overview

The **Network** menu has the options that you use to do the following tasks:

- Define TCP/IP settings, including DHCP or BOOTP server settings, when one of those types of servers is used to provide the required TCP/IP values
- Use the Ping utility
- Define and display settings that affect the Management Card's settings for DNS, FTP, Telnet, SSH, SNMP, E-mail, Syslog, and the Web interface (SSL/TLS)

Only an Administrator has access to the **Network** menu.

Menu options

Unless noted, the following menu options are available in the control console and Web interface:

- TCP/IP
- DNS
- Send DNS Query (Web interface)
- Ping utility (control console)
- FTP Server
- Telnet/SSH
- SNMP
- Email
- Syslog
- Web/SSL/TLS

Option Settings

TCP/IP

This option accesses the following settings:

- A Boot mode setting selects the method used to define the TCP/IP values that a Management Card needs to operate on the network:
  - **System IP**: The IP address of the Management Card
  - **Subnet Mask**: The subnet mask value
  - **Default Gateway**: The IP address of the default gateway

For information about the watchdog role the default gateway plays, see Resetting the network timer; for information about how to configure the initial TCP/IP settings when you install the Management Card, see the Network Management Card *Installation and Quick Start Manual* **(.\doc\insguide.pdf)**, provided on the APC Network Management Card *utility* CD and in printed form.

- Advanced settings define the Management Card's host and domain names, as well as TCP/IP port, BOOTP, and DHCP settings used by the Management Card.

Current TCP/IP settings fields. The current values for **System IP**, **Subnet Mask**, and **Default Gateway**, and the Management Card's **MAC Address**, **Host Name**, **Domain Name**, and **Ethernet Port Speed** values are displayed above the TCP/IP settings in the control console and the Web interface.

Boot mode setting. This setting selects which method will be used to define the Management Card's TCP/IP settings whenever the Management Card turns on, resets, or restarts:

- **Manual**: Three settings (**System IP**, **Subnet Mask**, and **Default Gateway**) which are only available when **Manual** is used to define the needed TCP/IP settings.
- **BOOTP only**: A BOOTP server provides the TCP/IP settings.
- **DHCP only**: A DHCP server provides the TCP/IP settings.
- **DHCP & BOOTP**: The Management Card will attempt to get its TCP/IP settings from a BOOTP server first, and then, if it cannot discover a BOOTP server, from a DHCP server.

An **After IP Assignment** setting, by default, will switch **Boot mode** from its default **DHCP & BOOTP** setting to **BOOTP only** or **DHCP only**, depending on the type of server that supplied the TCP/IP settings to the Management Card. For information about the **After IP Assignment** setting, and other settings that affect how the Management Card uses BOOTP and DHCP, see Advanced settings; For more information about how to use DHCP, see Boot Mode; for more information about how to use BOOTP, see the *Management Card Addendum* (**./doc/addendum.pdf**) provided on the APC Network Management Card *utility* CD.

Advanced settings. The boot mode affects which settings are available:

- Two settings are available for all **Boot mode** selections to define the Management Card's **Host Name** and **Domain Name** values.
- A **Port Speed** setting is available for all **Boot mode** selections to define the TCP/IP port's communication speed (**Auto-negotiate**, by default).
- Three settings are available for all **Boot mode** selections, except **Manual**, to identify the Management Card in BOOTP or DHCP communication:
  - **Vendor Class**: Uses **APC**, by default.
  - **Client ID**: Uses the Management Card's MAC address, by default.

If the **Client ID** is changed from the Management Card's MAC address, the new value must be unique on the LAN. Otherwise, the DHCP or BOOTP server may act incorrectly.

  - **User Class**: Uses the Management Card's application module type, by default. For example, a Symmetra module sets the **User Class** to **SY**, and a Smart-UPS/Matrix-UPS module sets it to **SUMX**.
- Two settings are available if **BOOTP only** is the Boot mode selection:
  - **Retry Then Fail**: Defines how many times the Management Card will attempt to discover a BOOTP server before it stops (4, by default).
  - **On Retry Failure**: Defines what TCP/IP settings will be used by the Management Card when it fails to discover a BOOTP server (**Use Prior Settings**, by default).

For information about the **Advanced** settings (**DHCP Cookie Is** and **Retry Then Stop**) that directly affect how DHCP is used, see Boot Mode.

DNS

Use this option to define the IP addresses of the primary and secondary Domain Name Servers (DNS) used by the Management Card's e-mail feature.

See E-mail Feature and DNS servers.

Send DNS Query (Web interface). Use this option, available only through the **DNS** menu in the Web interface, to send a DNS query that tests the setup of your DNS servers.

Use the following settings to define the parameters for the test DNS request; you view the result of the test DNS request in the **Last Query Response** field (**Passed**, **Failed**, or **Not Responding**).

- Use the **Query Type** setting to select the method to use for the DNS query:
  - The URL name of the server (**Name**)
  - The IP address of the server (**IP**)
  - The Mail Exchange used by the server (**MX**)
- Use the **Query Question** text field to identify the value to be used for the selected **Query Type**:
  - For **Name**, identify the URL
  - For **IP**, identify the IP address
  - For **MX**, identify the Mail Exchange address
- Use the **DNS Server to Query** to select whether you want to query the primary DNS server or secondary DNS server.

Ping utility (control console)

Select this option, available only in the control console, to check the Management Card's network connection by testing whether a defined IP address responds to the Ping network utility.

By default, the default gateway IP address (see TCP/IP) is used. However, you can use the IP address of any device known to be running on the network.

FTP Server

Use the **Access** setting to enable or disable the FTP server. The server is enabled by default.

FTP transfers files without using encryption. For higher security, use Secure CoPy (SCP) for file transfers. When you select and configure Secure SHell (SSH), SCP is enabled automatically. To configure SSH, see Telnet/SSH. If you decide to use SCP for file transfer, be sure to disable the FTP server.

Use the **Port** setting to identify the TCP/IP port that the FTP server uses for communications with the Management Card. The default **Port** setting is **21**.

You can change the **Port** setting to any unused port from **5000** to **32768** to enhance the protection provided by **User Name** and **Password** settings. You must then use a colon (:) in the command line to specify the non-default port. For example, for a port number of 5000 and a Management Card IP address of 159.215.12.114, you would use this command:

```
ftp 159.215.12.114:5000
```

To access a text version of the Management Card's event or data Log, see How to use FTP or SCP to retrieve log files.

To use FTP to download configuration files, see the *Management Card Addendum* (**./doc/addendum.pdf**) on the APC Network Management Card *utility* CD.

Telnet/SSH

Use the **Telnet/SSH** option to perform the following tasks:

- Enable or disable Telnet or the Secure SHell (SSH) protocol for remote control console access.
  - While SSH is enabled, you cannot use Telnet to access the control console.
  - Enabling SSH enables SCP automatically.

When SSH is enabled and its port and encryption ciphers configured, no further configuration is required to use SCP. (SCP uses the same configuration as SSH.)

  - Do not enable both versions of SSH unless you require that both be activated at the same time. (Security protocols use extensive processing power.)

To use SSH, you must have an SSH client installed. Most Linux and other UNIX® platforms include an SSH client as part of their installation, but Microsoft Windows operating systems do not. SSH clients are available from various vendors.

- Configure the port settings for Telnet and SSH.
- Select one or more data encryption algorithms for SSH, version 1, SSH version 2, or both.
- In the Web interface, specify a host key file previously created with the APC Security Wizard and load it to the Management Card.

From a command line interface, such as the command prompt on Windows operating systems, you can use FTP or Secure CoPy (SCP) to transfer the host key file. You must transfer the file to location **/sec** on the Management Card.

If you do not specify a host key file, the Network Management Card generates an RSA host key of 768 bits, instead of the 1024-bit RSA host key that the Wizard creates. **The Management Card can take up to 5 minutes to create this host key, and SSH is not accessible during that time.**

- Display the *fingerprint* of the SSH host key for SSH versions 1 and 2. Most SSH clients display the fingerprint at the start of a session. Compare the fingerprint displayed by the client to the fingerprint that you recorded from the Web interface or control console of the Management Card.

If you are using SSH version 2, expect a noticeable delay when logging on to the control console of the Management Card. Although the delay is not long, it can be mistaken for a problem because there is no explanatory message.

Option	Description
Telnet/SSH Network Configuration	
Access	Enables or disables the access method selected in **Protocol Mode**. **NOTE:** Enabling SSH automatically disables Telnet. To enable SSH, change the setting and then click **Next>>** in the Web interface or choose **Accept Changes** in the control console. You must then agree to the license agreement that is displayed
Protocol Mode	Choose one of the following: • **Telnet:** User names, passwords, and data are transmitted without encryption. • **Secure SHell (SSH), version 1:** User names, passwords and data are transmitted in encrypted form. There is little or no delay when you are logging on. • **Secure SHell (SSH), version 2:** User names, passwords and data are transmitted in encrypted form, but with somewhat more protection than version 1 from attempts to intercept, forge, or alter data during data transmission. There is a noticeable delay when you are logging on to the Management Card. • **Secure SHell (SSH), versions 1 and 2**: Do not enable both versions of SSH unless you require that both be activated at the same time. (Security protocols use extensive processing power.)

Option	Description
Telnet/SSH Port Configuration	

Telnet Port	Identifies the TCP/IP port used for communications by Telnet with the Management Card. The default is **23**.
	
	You can change the **Port** setting to the number of any unused port between **5000** and **32768** to enhance the protection provided by **User Name** and **Password** settings. Then, according to the requirements of your Telnet client program, you must use either a colon (:) or a space in the command line to specify the non-default port number. For example, for a port number of 5000 and a Management Card IP address of 159.215.12.114, your Telnet client would require one or the other of the following commands:
	
	`telnet 159.215.12.114:5000`
	
	`telnet 159.215.12.114 5000`

SSH Port	Identifies the TCP/IP port used for communications by the Secure SHell (SSH) protocol with the Management Card. The default is **22**. You can change the **Port** setting to the number of any unused port between **5000** and **32768** to enhance the protection provided by **User Name** and **Password** settings. See the documentation for your SSH client for information on the command line format required to specify a non-default port number when starting SSH.

Option	Description
SSH Server Configuration	
SSHv1 Encryption Algorithms	Enables or disables **DES**, and displays the status (always enabled) of **Blowfish**, two encryption algorithms (block ciphers) compatible with SSH, version 1, clients. • **DES**: The key length is 56 bits. • **Blowfish**: The key length is 128 bits. You cannot disable this algorithm. **NOTE:** Not all SSH clients can use every algorithm. If your SSH client cannot use **Blowfish**, you must also enable **DES**.
SSHv2 Encryption Algorithms	Enables or disables the following encryption algorithms (Block Ciphers) that are compatible with SSH version 2 clients. • **3DES** (enabled by default): The key length is 168 bits. • **Blowfish** (enabled by default): The key length is 128 bits. • **AES 128**: The key length is 128 bits. • **AES 256**: The key length is 256 bits. **NOTE:** Not all SSH clients can use every algorithm. Your SSH client selects the algorithm that provides the highest security from among the enabled algorithms that it is able to use. (If your SSH client cannot use either of the default algorithms, you must enable an AES algorithm that it can use.)

Option	Description
SSH User Host Key File	
Status:	The **Status** field Indicates the status of the host key (*private* key). In the control console, you display host key status by selecting **Advanced SSH Configuration**. • **SSH Disabled: No host key in use**: No host key has been transferred to the Management Card or a host key has been transferred improperly. **NOTE:** A host key must be installed to the **/sec** directory of the Management Card • **Generating**: The Management Card is generating a host key because no valid host key was installed in its **/sec** directory. • **Loading**: A host key is being loaded (i.e., being activated on the Management Card). • **Valid**: The host key is valid. (If you install an invalid host key, the Management Card discards it and generates a valid one. However, a host key that the Management Card generates is only 768 bits in length. A valid host key created by the APC Security Wizard is 1024 bits.)
Filename:	You can create a host key file with the APC Security Wizard and then upload it to the Management Card by using the Web interface. Use the **Browse** button for the **Filename** field to locate the file, then click **Apply**. Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the host key file to the Management Card. **NOTE:** Creating and uploading a host key in advance reduces the time required to enable SSH. If no host key is loaded when you enable SSH, the Management Card creates one when it reboots. **The Management Card takes up to 5 minutes to create this key, and the SSH server is not accessible during that time.**

Option	Description
SSH Host Key Fingerprint	
SSH v1:	Displays the SSH version 1 fingerprint for the host key. The fingerprint is a unique identifier to further authenticate the host key. In the control console, choose **Advanced SSH Configuration** and then **Host Key Information** to display the fingerprint.
SSH v2:	Displays the SSH version 2 fingerprint for the host key. The fingerprint is a unique identifier to further authenticate the host key. In the control console, choose **Advanced SSH Configuration** and then **Host Key Information** to display the fingerprint.

SNMP

An **Access** option (**Settings** in the control console) enables (by default) or disables SNMP. When SNMP is enabled, the **Access Control** settings allow you to control how each of the four available SNMP channels is used.

To define up to four NMSs that will serve as trap receivers, see Trap Receivers; to use SNMP to manage a UPS or an environmental monitor, see the *PowerNet® SNMP Management Information Base (MIB) Reference Guide* (**.\doc\mibguide.pdf**) on the APC Network Management Card *utility* CD.

Setting	Definition	
Community Name	This setting defines the password (maximum of 15 characters) which an NMS that is defined by the **NMS IP** setting uses to access the channel.	
NMS IP	Limits access to the NMSs specified by the format used for the IP address. • 159.215.12.1 allows only the NMS with that IP address to have access. • 159.215.12.255 allows access for any NMS on the 159.215.12 segment. • 159.215.255.255 allows access for any NMS on the 159.215 segment. • 159.255.255.255 allows access for any NMS on the 159 segment. • 0.0.0.0 or 255.255.255.255 allows access for any NMS.	
Access Type	Selects how the NMS defined by the NMS IP setting can use the channel, when that NMS uses the correct **Community Name**.	
	Read	The NMS can use GETs at any time, but it can never use SETs.
	Write	The NMS can use GETs at any time, and can use SETs when no one is logged into either the control console or Web interface.
	Disabled	The NMS cannot use GETs or SETs.
	Write+	The NMS can use GETs and SETs at any time, even when someone is logged into the control console or Web interface.

Email

You use this option to define two SMTP settings (**SMTP Server** and **From Address**) used by the Management Card's e-mail feature.

See SMTP settings and E-mail Feature.

Syslog

By default, the Management Card can send messages to up to four Syslog servers whenever Management Card, environmental monitor, or UPS events occur. The Syslog servers, which must be specifically identified by their IP addresses, record the events in a log that provides a centralized record of events that occur at network devices.

This user's guide does not describe Syslog or its configuration values in detail. For more information about Syslog, see RFC3164, at **www.ietf.org/rfc/rfc3164**.

Syslog settings. Leave the Syslog settings, except the **Server IP** settings, set to their defaults unless otherwise specified by the Syslog network or system administrator.

Setting	Definition
General Settings	
Access (Web interface) Syslog (control console)	Enables (by default) or disables the Syslog feature.
Facility	Selects the facility code assigned to the Management Card's Syslog messages (**User**, by default). **NOTE:** Although several daemon-specific and process-specific selections are available, along with eight generic selections, **User** is the selection that best defines the Syslog messages sent by a Management Card.

Setting	Definition
Syslog Server Settings	
Server IP	Uses specific IP addresses to Identify which of up to four servers will receive Syslog messages sent by the Management Card. **NOTE:** To use the Syslog feature, at least **Server IP** must be defined for at least one server.
Port	Identifies the user datagram protocol (UDP) port that the Management Card will use to send Syslog messages. The default is **514**, the number of the UDP port assigned to Syslog.
Local Priority (Severity Mapping)	
Map to Syslog's Priorities	Maps each of the severity levels (**Local Priority** settings) that can be assigned to UPS, environmental monitor, and Management Card events to the available Syslog priorities. The following definitions are from RFC3164: • **Emergency**: The system is unusable • **Alert**: Action must be taken immediately • **Critical**: Critical conditions • **Error**: Error conditions • **Warning**: Warning conditions • **Notice**: Normal but significant conditions • **Informational**: Informational messages • **Debug**: Debug-level messages Following are the default settings for the four **Local Priority** settings: • **Severe** is mapped to **Critical** • **Warning** is mapped to **Warning** • **Informational** is mapped to **Info** • **None** (for events that have no severity level assigned) is mapped to **Info** **NOTE:** To disable sending Syslog messages for **Severe**, **Warning**, or **Informational** events, see Event Actions (Web Interface Only).

Syslog test (Web interface). This option allows you to send a test message to the Syslog servers configured in the **Syslog Server** section.

1. Select the **Priority** you want to assign to the test message.
2. Define the **Test Message** using any text that meets the format described in Syslog message format below. For example, `APC: Test message`, meets the required message format.
3. Click **Apply** to have the Management Card send a Syslog message that uses the defined **Priority** and **Test Message** settings.

Syslog message format. A Syslog message has three parts:

- The priority (PRI) part identifies the Syslog priority assigned to the message's event and the facility code assigned to messages sent by the Management Card.
- The Header includes a time stamp and the IP address of the Management Card.
- The message (MSG) part has two fields:
  - A TAG field, which is followed by a colon and a space, identifies the event type (APC, System, or UPS, for example)
  - A CONTENT field provides the event text, followed by a space and the event code

Web/SSL/TLS

Use the **Web/SSL/TLS** menu to perform the following tasks.

- Enable or disable the two protocols that provide access to the Web interface of the Network Management Card:
  - Hypertext Transfer Protocol (HTTP) provides access by user name and password, but does not encrypt user names, passwords, and data during transmission.
  - Hypertext Transfer Protocol over Secure Socket Layer (HTTPS). Secure Socket Layer (SSL) encrypts user names, passwords, and data during transmission and provides authentication of the Network Management Card by means of digital certificates.

    See Creating and Installing Digital Certificates to choose among the several methods for using digital certificates.

- Configure the ports that each of the two protocols will use.
- Select the encryption ciphers that SSL will use.
- Identify whether a server certificate is installed on the Management Card. If a certificate has been created with the APC Security Wizard but is not installed:
  - In the Web interface, browse to the certificate file and upload it to the Management Card.
  - Alternatively, use the Secure CoPy (SCP) protocol or FTP to upload it to the location **\sec** on the Management Card

Note

Creating and uploading a server certificate in advance reduces the time required to enable HTTPS (SSL/TLS). If no server certificate is loaded when you enable HTTPS (SSL/TLS), the Management Card creates one when it reboots. **The Management Card can take up to 5 minutes to create this certificate, and the SSL/TLS server is not available during that time.**

- Display the configured parameters of a digital server certificate, if one is installed.

Option	Description
Web/SSL/TLS Network Configuration	
Access	Enables or disables the access method selected in **Protocol Mode**.
Protocol Mode	Choose one of the following: • **HTTP:** User names, passwords, and data are transmitted without encryption. • **HTTPS (SSL/TLS):** User names, passwords and data are transmitted in encrypted form, and digital certificates are used for authentication. **NOTE:** To enable HTTPS (SSL/TLS), change the setting and then click **Next>>** in the Web interface, or choose **Accept Changes** in the control console. You must then agree to the license agreement that is displayed. To activate the changes you must log off and log back on to the interface. When SSL is activated, your browser displays a lock icon, usually at the bottom of the screen. 

Option	Description
HTTP/HTTPS Port Configuration	
HTTP Port	Identifies the TCP/IP port used for communications by HTTP with the Management Card. The default is **80**. You can change the **Port** setting to the number of any unused port between **5000** and **32768** to enhance the protection provided by **User Name** and **Password** settings. You must then use a colon (:) in the command line to specify the non-default port number. For example, for a port number of 5000 and a Management Card IP address of 159.215.12.114, you would use this command: `http://159.215.12.114:5000`
HTTPS Port	Identifies the TCP/IP port used for communications by HTTPS with the Management Card. The default is **443**. You can change the **Port** setting to the number of any unused port between **5000** and **32768** to enhance the protection provided by **User Name** and **Password** settings. You must then use a colon (:) in the command line to specify the non-default port number. For example, for a port number of 6502 and a Management Card IP address of 159.215.12.114, you would use this command: `https://159.215.12.114:6502`

Option	Description
SSL/TSL Server Configuration	
CipherSuite	Enables or disables the following SSL encryption ciphers and hash algorithms. (To access these options in the control console, choose **Web/SSL/TLS**, then **Advanced SSL/TLS Configuration**.) **NOTE:** All of these encryption ciphers and hash algorithms use the RSA public key algorithm. • **DES (SSL_RSA_WITH_DES_CBC_SHA)**: a block cipher with a key length of 56 bits. The Secure Hash Algorithm (SHA) is used for authentication. • **3DES (SSL_RSA_WITH_3DES_EDE_CBC_SHA)**: a block cipher with a key length of 168 bits. A Secure Hash Algorithm (SHA) is used for authentication. • **RC4 (SSL_RSA_WITH_RC4_128_MD5)**: a stream cipher with a key length of 128 bits, with an RSA key exchange algorithm, and with a Message Digest 5 (MD5) hash algorithm used for authentication. This selection is enabled by default. • **RC4 (SSL_RSA_WITH_RC4_128_SHA)**: a stream cipher with a key length of 128 bits. A Secure Hash Algorithm (SHA) is used for authentication. This selection is enabled by default.

Option	Description
SSL/TLS Server Certificate	
Status:	The **Status** field indicates whether a server certificate is installed. (To display the status in the control console, choose **Web/SSL/TLS**, then **Advanced SSL/TLS Configuration**.) • **Not installed**: No certificate is installed on the Management Card. **NOTE:** If you install a certificate by using FTP or SCP, you must specify the correct location (**/sec**) on the Management Card. • **Generating**: The Management Card is generating a certificate because no valid certificate was installed. • **Loading**: A certificate is being loaded (activated on the Management Card). • **Valid**: A valid certificate was installed to or generated by the Management Card. (If you install an invalid certificate, the Management Card discards it and generates a valid one. However, a certificate that the Management Card generates has some limitations. See Method 1: Use APC's default certificate.)
Filename:	You can create a server certificate with the APC Security Wizard and then upload it to the Management Card by using the Web interface. Use the **Browse** button for the **Filename** field to locate the file, then click **Apply**. By default, the certificate is installed to the correct location. Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the server certificate to the Management Card. However, you must specify the correct location (**/sec**) on the Management Card. **NOTE:** Creating and uploading a server certificate in advance reduces the time required to enable HTTPS (SSL/TLS). If no server certificate is loaded when you enable HTTPS (SSL/TLS), the Management Card creates one when it reboots. **The Management Card can take up to 5 minutes to create this certificate, and the SSL/TLS server is not available during that time**.

Parameter	Description
Current Certificate Details	
Issued to:	**Common Name (CN)**: The IP Address or DNS name of the Management Card, except if the server certificate was generated by default by the Management Card. For a default server certificate, the **Common Name (CN)** field displays the Management Card's serial number. **NOTE:** If an IP address was specified as the Common Name when the certificate was created, use an IP address to log on to the Web interface of the Management Card; if the DNS name was specified as the Common Name, use the DNS name to log on. When you log on, if you do not use the IP address or DNS name that was specified for the certificate, authentication fails, and you receive an error message asking if you want to continue. **Organization (O)**, **Organizational Unit (OU**), and **Locality, Country:** The name, organizational unit, and location of the organization that is using the server certificate. If the server certificate was generated by default by the Management Card, the **Organizational Unit (OU)** field displays "Internally Generated Certificate." **Serial Number**: The serial number of the server certificate.
Issued By:	**Common Name (CN)**: The Common Name as specified in the CA root certificate, except if the server certificate was generated by default by the Management Card. For a default server certificate, the **Common Name (CN)** field displays the Management Card's serial number. **Organization (O)** and **Organizational Unit (OU**): The name and organizational unit of the organization that issued the server certificate. If the server certificate was generated by default by the Management Card, the **Organizational Unit (OU)** field displays "Internally Generated Certificate."
Validity	**Issued on**: The date and time at which the certificate was issued. **Expires on**: The date and time at which the certificate expires.

Parameter	Description
Fingerprints	Each of the two fingerprints is a long string of alphanumeric characters punctuated by colons. A fingerprint is a unique identifier that you can use to further authenticate the server. Record the fingerprints to compare with the fingerprints contained in the certificate, as displayed in the browser. **SHA1 Fingerprint**: This fingerprint is created by a Secure Hash Algorithm (SHA). **MD5 Fingerprint**: This fingerprint is created by a Message Digest 5 (MD5) algorithm.

System Menu

Introduction

Overview

The **System** menu has the options that you use to do the following tasks:

- Configure system identification, date and time settings, and access parameters for the Administrator, Device Manager, and Read Only User accounts.
- Synchronize the Management Card's real-time clock with a Network Time Protocol (NTP) server.
- Download configuration files.
- Reset or restart the Management Card.
- Define the URL links available in the Web interface.
- Access hardware and firmware information about the Management Card.
- Set the units (Fahrenheit or Celsius) used for temperature displays.
- Configure dial-in access to the control console at an AP9618 Network Management Card using the Management Card's internal analog modem.

Only an Administrator has access to the **System** menu.

Menu options

Unless noted, the following menu options are available in the control console and Web interface:

- User Manager
- Identification
- Date & Time
- Tools
- Modem (AP9618 control console)
- Preferences (Web interface)
- Links (Web interface)
- About System

About System is an option of the **Help** menu in the Web interface.

Option Settings

User Manager

Use this option to define the access values shared by the control console and the Web interface, and the authentication used to access the Web interface.

Setting	Definition
Values affecting all users	
Auto Logout	The number of minutes (3 by default) before a user is automatically logged off because of inactivity.
Authentication	The **Basic** setting (default) causes the Web interface to use standard HTTP 1.1 login (base64-encoded passwords); **MD5** causes the Web interface to use an MD5-based authentication login. **NOTE:** Cookies must be enabled at a browser before it can be used with MD5 authentication.
Separate values for Administrator, Device Manager, and Read Only User	
User Name	The case-sensitive name (maximum of 10 characters) used by Administrator and Device Manager users to log on at the control console or Web interface, and by the Read Only User to log on at the Web interface only. • **apc**, by default, for **Administrator** • **device**, by default, for **Device Manager** • **readonly**, by default, for the **Read Only User**.
Password	The case-sensitive password (maximum of 10 characters) always used to log on at the control console, but only used to log on to the Web interface when **Basic** is selected for the **Authentication** setting (**apc** is the default for the **Password** settings for the three account types). **NOTE:** A Read Only User is not permitted to log on through the control console.
Authentication Phrase	The case-sensitive, 15-to-32 character phrase used to log on to the Web interface when MD5 is the **Authentication** setting. The default settings are: • **admin user phrase** for **Administrator** • **device user phrase** for **Device Manager** • **readonly user phrase** for **Read Only User**

Identification

Use this option to define the System **Name**, **Location**, and **Contact** values used by the Management Card's SNMP agent. The option's settings provide the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifications (OIDs).

For more information about the MIB-II OIDs, see the PowerNet® *SNMP Management Information Base (MIB) Reference Guide* (**./doc/mibguide.pdf**) provided on the APC Network Management Card *utility* CD.

Date & Time

Use this option to set the time and date used by the Management Card. The option displays the current settings, and allows you to change those settings manually, or through a Network Time Protocol (NTP) Server.

Set Manually. Use this option in the Web interface, or **Manual** in the control console, to define the date and time for the Management Card.

Note

An **Apply Local Computer Time to Network Management Card** option, which is available in the Web interface only, sets these values to match the date and time settings of the computer you are using to access the Web interface.

Synchronize with Network Time Protocol (NTP) Server. Use this option, or **Network Time Protocol (NTP)** in the control console, to have an NTP Server update the date and time for the Management Card automatically.

Note

In the control console, use the **NTP Client** option to enable or disable (the default) the NTP Server updates. In the Web interface, use the **Set Manually** option to disable the updates.

Setting	Definition
Primary NTP Server	Identifies the IP address of the primary NTP server.
Secondary NTP Server	Identifies the IP address of the secondary NTP server, when a secondary server is available.
GMT Offset (Time Zone)	Defines the offset from Greenwich Mean Time (GMT) based on the Management Card's time zone.
Update Interval	Defines how often, in hours, the Management Card accesses the NTP Server for an update. The minimum is 1 hour; the maximum is 8760 hours (1 year). Use **Update Using NTP Now** to initiate an immediate update as well.

Tools

Use this option to restart the Management Card or to reset some or all of its configuration settings to their original, default values.

Action	Definition
Reboot Card	Restarts the Management Card.
Reset Card to Defaults	Resets all configuration settings. **NOTE:** For information about how this affects the **Boot mode** setting, see this table's description of **Reset Only TCP/IP to Defaults**.
Reset Card to Defaults Except TCP/IP	Resets all configuration settings except the TCP/IP settings.
Reset Only TCP/IP to Defaults	Resets the TCP/IP settings only. **NOTE:** WIth **Boot mode** set to **DHCP & BOOTP**, its default setting, the Management Card's TCP/IP settings must be defined by a DHCP or BOOTP server. See TCP/IP.
Delete SSH Host Keys and SSL Certificates	Removes any SSH host key and server certificate on the Management Card so that you can reconfigure these components of your security system.
XMODEM (control console only)	Allows you to download firmware using a terminal-emulation program when you use a local connection to the control console only. For more information about how you connect to the control console locally, see Local access to the control console.

Preferences (Web interface)

Use this option to define whether temperature values are displayed as Fahrenheit or Celsius in the Web interface and the control console.

Links (Web interface)

Use this option to modify the links to APC Web pages.

Setting	Definition
User Links	
Name	Defines the link names that appear in the **Links** menu (by default, **APC's Web Site**, **Testdrive Demo**, and **APC Monitoring**).
URL	Defines the URL addresses used by the links. By default, the following URL addresses are used: • **http://www.apc.com** (**APC's Web Site**) • **http://testdrive.apc.com** (**Testdrive Demo**) • **http://rms.apc.com** (**APC Monitoring**) **NOTE:** For information about these pages see Links menu.
Access Links	
APC Home Page	Defines the URL address used by the APC logo at the top of all Web interface pages (by default, **http://www.apc.com**).

Modem (AP9618 control console)

Use this option, which is available in the AP9618 Network Management Card's control console only, to configure dial-in access to the control console using the Management Card's internal analog modem.

Setting	Definition
Console Dial-In	Enables (by default) or disables dial-in access to the control console through the analog modem.
Initialization	Defines the initialization string used to ensure proper operation of the modem, and consistent communication between the modem and the Management Card. This string is sent to the Management Card's internal modem every time the Management Card restarts, or when a setting change is made and accepted.
Country Code	Identifies the country in which the modem is used to match the modem's operation to that country's telephone-system standards.
Terminal Interface	Allows an advanced user to send commands directly to the modem and view the modem's response, using a serial, terminal-interface session at 38400 baud. When CTRL+A is used to end the session, the modem is reset to use the **Initialization** setting described above.

About System

This option identifies hardware information for the Management Card, including **Model Number**, **Serial Number**, **Manufacture Date**, **Hardware Revision**, **MAC Address**, and **Flash Type.**

The hardware information will never change. For example, if you use an AP9168U upgrade kit to convert an AP9617 Network Management Card *EX* to an AP9618 Network Management Card *EM/MDM*, the **About System** option still reports **AP9617** for that Management Card's model number.

In the Web interface, except for **Flash Type**, this hardware information is reported by the **About System** option in the **Help** menu.

UPS Menu

Introduction

Overview

In the Web interface, the UPS menu is in the navigation menu; in the control console, you access the UPS menu through the **Device Manager** option in the **Control Console** menu. The menu is named with the model name of the UPS you are using.

UPS menu options

The UPS menu options and the information they provide vary by UPS model.

For information about the UPS menu options available in both the control console and the Web interface, see the following:

- UPS Status
- Diagnostics
- Control
- Configuration
- Module Status (Symmetra UPS or Symmetra PX UPS)
- Scheduling (UPS Shutdown)

A Silcon UPS has no **Diagnostics** or **Scheduling** options.

UPS Status

Overview

The **Status** options provide access to the information described in the following sections:

- Detailed UPS Status
- Utility Power Status
- Output Power Status
- Fault Tolerance (Symmetra or Symmetra PX UPS)
- Battery Status

For a Silcon UPS, the “Status of UPS” page in the Web interface includes the **View the refreshing status page** hyperlink described in Configure Parallel UPS parameters (Silcon UPS only).

Detailed UPS Status

In the Web interface, use the **Status** option in the UPS menu to access the following UPS status information; in the control console, this status information is listed above the UPS menu.

- The current status of the UPS.

For a list of the UPS events that can be reported as part of the UPS status, see "Event List" page.

The UPS menu in the control console has a **Detailed Status** option (Smart-UPS or Matrix-UPS) or **Detailed UPS Information** option (Symmetra or Silcon UPS) that accesses expanded descriptions of the UPS status. In addition, for Symmetra UPS models, a **Faults & Alarms** option accesses descriptions of any faults or alarms reported.

- The reason for the last transfer to battery power at the UPS
- The internal temperature of the UPS
- The runtime that is available currently to the UPS
- The values described in Utility Power Status, Output Power Status, and Battery Status
- The Fault tolerance parameters described in Fault Tolerance (Symmetra or Symmetra PX UPS)

For information about the conditions that are mapped to the non-specific faults that a Silcon UPS can report, see the file **dp3etrap.pdf** in the **.\help\dp3e** folder on the APC Network Management Card *utility* CD.

Utility Power Status

Footnotes indicate which utility-power fields are shared by which UPS models. (If no footnote is used, all UPS models report that value.)

A 3-phase UPS (Symmetra PX UPS or Silcon UPS) identifies the values for all three phases.

Status Field	Definition
Bypass Input Voltage[1]	The AC voltage (VAC) used when the UPS is in bypass mode.
Input Current[1]	The current, in Amps, supplied by the input voltage.
Input Frequency[2]	The input voltage's frequency, in Hertz (Hz). **NOTE:** In the control console for Smart-UPS or Matrix-UPS, the **Operating Frequency** field reports the frequency value shared by the input and output voltages.
Input Voltage	The AC voltage (VAC) being input to the UPS.
Minimum Line Voltage	The lowest AC voltage input to the UPS during the previous minute of operation.
Maximum Line Voltage	The highest AC voltage input to the UPS during the previous minute of operation.

1 Symmetra PX UPS and Silcon UPS models
2 Smart-UPS, Matrix-UPS, or Symmetra UPS models

Output Power Status

Footnotes to indicate which output-power fields are shared by which UPS models.

The Smart-UPS product line has a wide variety of models. If a status field is listed for Smart-UPS in the table, it may be supported on only some Smart-UPS models.

Only the status field **Output Voltage** is shared by all UPS models.

A 3-phase UPS (Symmetra PX UPS or Silcon UPS) identifies the values for all three phases.

Status Field	Definition
Load Current[1, 2] or Output Current[3]	The current, in Amps, supplied to the load.
Load Power[1, 2]	The UPS load as a percentage of available Watts.
Apparent Load Power[1, 2]	The UPS load as a percentage of available VA.
Output Frequency[4]	The frequency, in Hz, used by the output voltage. In the control console for Smart-UPS or Matrix-UPS, the **Operating Frequency** field reports the frequency value shared by the input and output voltages.
Output kVA[5] or Output Power[6]	The load placed on each phase by the attached equipment, in total kVA.
Output Power Percentage[6]	The load placed on each phase by the attached equipment, expressed as a percentage of the available kVA.
Output VA at n+0[7]	The load placed on each phase by the attached equipment, as a percentage of the VA available with no redundancy.
Output VA at n+1[7]	The load placed on each phase by the attached equipment, as a percentage of the VA available with the identified redundancy.
Output Voltage	The AC voltage the UPS is providing to its load.
Output Watts at n+0[7]	The load placed on each phase by the attached equipment, as a percentage of the Watts available with no redundancy.
Output Watts at n+1[7]	The load placed on each phase by the attached equipment, as a percentage of the Watts available with the identified redundancy.
Peak Output Current[8]	The highest current, in Amps, output by each phase.

1 Matrix-UPS
2 Smart-UPS
3 Symmetra, Symmetra PX UPS, or Silcon UPS
4 Smart-UPS, Matrix-UPS, or Symmetra UPS
5 Symmetra PX UPS
6 Silcon UPS
7 Symmetra or Symmetra PX UPS
8 Symmetra PX UPS or Silcon UPS

Fault Tolerance (Symmetra or Symmetra PX UPS)

Note

In the control console, use the **Detailed UPS Information** option to access the fault tolerance status.

Status Field	Definition
Present KVA Capacity	The maximum load that the Symmetra can support.
Redundancy	The number of power modules which can fail or be removed without causing the Symmetra to switch to bypass.

Battery Status

Footnotes indicate which output-power fields are shared by which UPS models. Only the status field **Runtime Remaining** is shared by all UPS models.

Status Field	Definition
Battery Capacity[1]	How much of the UPS battery capacity is available to support the attached equipment.
Battery Current[2]	The current being output from the battery.
Battery Voltage[3], Actual Battery Voltage[2], or Actual Battery Bus Voltage[4]	The available DC power.
Calibration Date[1]	When the last runtime calibration was performed.
Calibration Result[1]	The result of the last runtime calibration.
Nominal Battery Voltage[5]	The basic voltage range that the battery needs to supply when the UPS uses its battery for output power. This field appears only in the Web interface.
Number of Bad Batteries[1]	How many UPS batteries need replacing (reported only when the UPS has at least one external battery).
Number of Batteries[3] or Number of External Batteries[6]	How many batteries the UPS has.
Runtime Remaining	How long the UPS can use battery power to support its attached equipment.
Self-Test Result[1]	The result of the last self-test.
Self-Test Date[1]	When the last self-test was performed.

1 Smart-UPS, Matrix-UPS, Symmetra, or Symmetra PX UPS
2 Symmetra PX UPS or Silcon UPS
3 Smart-UPS or Matrix-UPS
4 Symmetra PX UPS
5 Symmetra, Symmetra PX UPS, or Silcon UPS
6 Symmetra or Symmetra PX UPS

Diagnostics

Overview

There are two types of diagnostics options you can use with all UPS models except a Silcon UPS, which has no diagnostic options:

- Options which cause a specified test to occur immediately
- A scheduling option which controls when a UPS self-test occurs

Diagnostic tests

In the Web interface, use the **Diagnostics** option of the UPS menu to perform diagnostic tests or to view the results of the last self-test or runtime calibration.

In the control console, the diagnostics options are in the **Control** menu.

Smart-UPS, Matrix-UPS, or Symmetra UPS. You can use diagnostics options to perform the following tests.

For the results of the last self-test and last runtime calibration:

- In the Web interface, use the "Diagnostics" page.
- In the control console, use the option **Detailed Status** (Smart-UPS or Matrix-UPS models) or **Detailed UPS Information** (Symmetra or Silcon UPS models).

Test	Definition
Self-Test	Perform a self-test of the UPS.
Simulate Power Failure	Causes the UPS to test its ability to switch to battery operation.
Start/Stop Runtime Calibration	Initiates (or cancels) a runtime calibration, a process which calculates how much runtime the UPS has available. **NOTE:** You can perform a runtime calibration only when the battery is at 100% capacity.
Test UPS Alarm (Smart-UPS or Matrix-UPS)	Causes a Matrix-UPS to generate an alarm tone, and a Smart-UPS to generate an alarm tone and flash its front panel lights. If the Smart-UPS is a member of a Synchronized Control Group: • In the Web interface, this option always tests the alarms of all enabled members of the group. • In the control console, you are prompted to choose whether to apply the action to the initiating UPS or to all members of the group. • In SNMP, you can set the OID **upsAdvControlFlashAndBeep** to either option: **flashAndBeep (2)** to test the alarm of an individual UPS or **flashAndBeepSyncGroup (3)** to test the alarms of all enabled group members.

Symmetra PX UPS. Use buttons on the "Diagnostics" page in the Web interface to perform self-tests (**Tests...**) or runtime calibrations (**Calibrate...**).

For the results of the last self-test and last runtime calibration, and the status of intelligence modules, power modules, batteries, and the communication bus and subsystems:

- In the Web interface, use the "Diagnostics" page.
- In the control console, use the **Detailed UPS Information** option.

Scheduled UPS self-tests

To schedule a self-test:

- In the Web interface, select **Diagnostics** on the UPS menu, then use the **Auto Self-Test** option.
- In the control console, from the UPS menu:
  - For Symmetra and Symmetra PX UPS models, select **Scheduled Tests**.
  - For Smart-UPS or Matrix-UPS models, select **Configuration**, **General**, and **Self-Test Schedule**.

The scheduling option allows you to control when a UPS self-test occurs. The available selections are **Never**, **UPS Startup**, **Every 7 Days**, or **Every 14 Days**.

Control

Initiating a UPS Control option

You can initiate a UPS Control option in either of these ways:

- For the UPS of the initiating Management Card only.
  - In the Web interface, select **No** for **Apply to Sync Group?**
  - In the control console, type **NO** (in uppercase) in response to the question **Apply command to all SCG members?**
- For all members of the Synchronized Control Group to which this Management Card belongs (if the option is allowed for Synchronized Control Groups).
  - In the Web interface, select **Yes** for **Apply to Sync Group?**
  - In the control console, press ENTER in response to the question **Apply command to all SCG members?**

The option to apply an action to a Synchronized Control Group is displayed only if this Management Card is an active (enabled) member of a Synchronized Control Group.

The following guidelines apply to Synchronized Control Groups:

- All UPSs in a Synchronized Control Group must be the same model.
- Synchronized Control Groups are supported for most UPS models of the Smart-UPS and Symmetra UPS product lines. Any Smart-UPS or Symmetra UPS with a card slot that accepts a Network Management Card supports Synchronized Control Groups.
- In a Synchronized Control Group of Symmetra 3-phase UPSs, the shutdown mode setting must be either normal or secure for each UPS.

To configure a Management Card to be a member of a Synchronized Control Group, see Sync Control.

The synchronization process . If you apply an action to the Synchronization Control Group, the UPSs with management cards that are enabled group members behave as follows:

- Each UPS receives the command regardless of its output status, even if it is in a low-battery state.
- The action uses the delay periods (such as **Shutdown Delay**, **Sleep Time**, and **Return Delay)** that are configured for the initiating UPS.
- When the action begins, a UPS that is unable to participate retains its present output status while the other UPSs in the group perform the action. If a UPS is already in the output state that the action requires (e.g., a UPS is already off when the **Reboot UPS** action starts), that UPS logs an event, but performs the rest of the action, if any.
- All UPSs participating in the action synchronize their performance of the action (within a one-second time period under ideal conditions for Smart-UPS, but sometimes longer, especially for Symmetra UPSs).
- In reboot and sleep actions:
  - Immediately before the initiating UPS begins its **Return Delay**, by default it waits up to 120 seconds (its configurable **Power Synchronized Delay**) for any UPS that does not have input power to regain that power. Any UPS that fails to regain input power within the **Power Synchronized Delay** does not participate in the synchronized restart, but instead waits until its own input power returns before restarting.
  - The LEDs on the front of the UPS do not sequence their lights as they do for a normal (not synchronized) reboot or sleep action.
- UPS status and events are reported in the same way for synchronized actions as for actions on individual UPSs.

For more information about the delays and required battery capacity settings in the following table see Configuration and Sync Control.

Actions (for a single UPS and Synchronized Control Groups).

You can use the actions described in the table on the next several pages for individual UPSs and for Synchronized Control Groups, within these guidelines:

- All actions except **Put UPS in Bypass** and **Take UPS Off Bypass**:
  - These actions are available for Synchronized Control Groups of Symmetra UPS or Smart-UPS models.
  - These actions are available for all individual APC UPSs except Silcon UPS models.

To control a Silcon UPS, see Control options for Silcon UPS.

- **Put UPS in Bypass** and **Take UPS Off Bypass**:
  - These actions are available only for individual UPSs, not for Synchronized Control Groups.
  - These actions are available only for Matrix-UPS, Symmetra UPS, and some Smart-UPS.

For descriptions of the UPS Control options **Self-Test**, **Simulate Power Failure**, **Start/Stop Runtime Calibration**, and **Test UPS Alarm**, see Diagnostic tests.

Action	Definition
Turn UPS On (control console)	This action turns on power at the UPS. For a Synchronized Control Group, after a delay of a few seconds, the action turns on all enabled group members that have input power.
Turn UPS Off	This action turns off power immediately at the UPS, without a shutdown delay, and the UPS remains off until you turn on its power again. If the UPS is a member of a Synchronized Control Group, this action turns off power at all UPSs that are enabled members of the group. No **Shutdown Delay** is used. The UPSs turn off after a few seconds, and they remain off until you turn on their power again. **NOTE:** For a synchronized turn-off action that uses the **Shutdown Delay** of the initiating UPS, use SNMP. Set the value **turnUpsSyncGroupOffAfterDelay (5)** for the **upsAdvControlUpsOff** OID.
Turn UPS Off Gracefully[1] (control console)	This action turns off power after the UPS's **Maximum Shutdown Time** plus two minutes, and its **Shutdown Delay**. For information about how the **Maximum Shutdown Time** is determined, see Maximum-Shutdown-Time negotiation. For a Synchronized Control Group, the action is performed using the delays configured for the group member that initiated the action.

1 When you select **Yes** for the Web interface's **Signal servers** option, initiating a **Turn UPS Off**, **Reboot UPS**, or **Put UPS To Sleep** action is equivalent to selecting **Turn UPS Off Gracefully**, **Reboot UPS Gracefully**, or **Put UPS To Sleep Gracefully** in the control console.

Action	Definition
Reboot UPS	This option restarts the attached equipment by doing the following: • Turns off power at the UPS after the **Shutdown Delay** • Turns on power at the UPS after the UPS battery capacity returns to at least the percentage configured for **Return Battery Capacity** and the UPS waits the time specified as **Return Delay**. For a Synchronized Control Group action: • This option turns off power at the UPSs that are enabled group members after waiting the time configured as the initiating UPSs **Shutdown Delay** • The initiating UPS then waits up to the number of seconds specified as **Power Synchronized Delay** to allow time for group members to regain input power. If all group members have already regained input power, this delay is omitted. If all group members regain input power during the delay, the remainder of the delay is cancelled. • The **Return Delay** then starts when the initiating UPS is at its configured **Return Battery Capacity**. • The **Return Battery Capacity** of the initiating UPS is also required of group members, but you can reduce the capacity required of a group member by configuring that member's **Return Battery Capacity Offset** (set at 10% by default). For example, if the initiator's **Return Battery Capacity** is set at 50%, and a member's **Return Battery Capacity Offset** is set to 5%, that member's battery capacity will need to be at only 45% for that member to reboot.
Reboot UPS Gracefully[1] (control console)	This action is performed similarly to the **Reboot UPS** action, but with an additional delay before the shutdown portion of the action. The attached equipment shuts down only after the UPS (or the initiating UPS for a Synchronized Control Group action) waits the **Maximum Shutdown Time** plus two minutes. For information about how the **Maximum Shutdown Time** is determined, see Maximum-Shutdown-Time negotiation.

1 When you select **Yes** for the Web interface's **Signal servers** option, initiating a **Turn UPS Off**, **Reboot UPS**, or **Put UPS To Sleep** action is equivalent to selecting **Turn UPS Off Gracefully**, **Reboot UPS Gracefully**, or **Put UPS To Sleep Gracefully** in the control console.

Action	Definition
Put UPS To Sleep	This option puts the UPS into sleep mode by turning off its output power for a defined period of time, as follows: • The UPS turns off output power after waiting the time configured as its **Shutdown Delay**. • When input power returns, the UPS turns on output power after two configured periods of time: its **Sleep Time** and **Return Delay**. • For a synchronized control group action, the Management Card of the UPS initiating the action waits up to the number of seconds configured as its **Power Synchronized Delay** for enabled group members to regain input power before it starts the **Return Delay**. If all group members have already regained input power, the **Power Synchronized Delay** is omitted. If all group members regain input power during the delay, the remainder of the delay is cancelled.
Put UPS To Sleep Gracefully[1] (control console)	This action puts the UPS into sleep mode (turns off power for a defined period of time), as follows: • The UPS turns off output power after waiting the delay times configured as its **Maximum Shutdown Time** plus 2 minutes (to allows time for PowerChute network shutdown to safely shut down its server) and its **Shutdown Delay**. • When input power returns, the UPS turns on output power after two configured periods of time: its **Sleep Time** and **Return Delay**. • For a synchronized control group action, the Management Card of the UPS initiating the action waits up to the number of seconds configured as its **Power Synchronized Delay** for enabled group members to regain input power before it starts the **Return Delay**. If all group members have already regained input power, the **Power Synchronized Delay** is omitted. If all group members regain input power during the delay, the remainder of the delay is cancelled
Put UPS In Bypass Take UPS Off Bypass	Controls the use of bypass mode, which allows maintenance to be performed at a Matrix-UPS, a Symmetra UPS, and some Smart-UPS models without turning off power at the UPS.

1 When you select **Yes** for the Web interface's **Signal servers** option, initiating a **Turn UPS Off**, **Reboot UPS**, or **Put UPS To Sleep** action is equivalent to selecting **Turn UPS Off Gracefully**, **Reboot UPS Gracefully**, or **Put UPS To Sleep Gracefully** in the control console.

Control options for Silcon UPS. By default, no control options are available for Silcon UPS.

To use control options for a Silcon UPS, you must enable the **Accept Remote Turn Off Commands** option, available only in the control console's **UPS Control** menu and only when you use a local, serial connection to access the control console.

To use a serial connection, see Local access to the control console.

When **Accept Remote Turn Off Commands** is enabled:

- Two control options, **Turn UPS Off** and **Turn UPS Off Gracefully** options, become available for a Silcon UPS
- A **Disable Remote Turn Off Commands** option is available in the **UPS Control** menu at the Web interface and control console, allowing you to disable using the Management Card to turn off the Silcon UPS

Configuration

Overview

The UPS menu's **Configuration** option provides access to the configurable parameters described in the following sections:

- Utility Line Settings
- Alarm Thresholds (Symmetra UPS or Symmetra PX UPS)
- Shutdown Parameters
- General Settings
- Reset UPS Defaults
- Configure Parallel UPS parameters (Silcon UPS only)

Utility Line Settings

This **Configuration** menu option is available to all UPS models except a Silcon UPS. The available settings differ based on the UPS model.

Smart-UPS or Matrix-UPS. Not all **Utility Line** settings are available for all Smart-UPS and Matrix-UPS models, and each setting's selections can differ by UPS model.

Setting	Definition
Output Voltage	The nominal AC voltage level for the UPS output.
High Transfer Voltage	The upper limit of acceptable input voltage. When the input reaches this value: • Matrix-UPS switches to battery operation • Smart-UPS starts to use its AVR Trim feature.
Low Transfer Voltage	The lower limit of acceptable input voltage. When the input reaches this value, Smart-UPS starts to use its AVR Boost feature or switches to battery operation if it does not have this feature. **NOTE:** For Matrix-UPS, this setting cannot be changed.
Bypass Upper Voltage	The input voltage above which the UPS cannot switch to bypass mode.
Bypass Lower Votage	The input voltage below which the UPS cannot switch to bypass mode.
Vout Reporting (Matrix-UPS)	How Matrix-UPS scales its output voltage readings.
Sensitivity	How sensitive the UPS will be to distortions in the input voltage. **NOTE:** Matrix-UPS always uses the **Automatic** setting.
Output Frequency Range	Defines the nominal value for the frequency used by the output voltage.

Symmetra or Symmetra PX UPS. The following table describes the **Utility Line** settings for a Symmetra UPS. A Symmetra PX UPS uses only the settings **Output Frequency Range** and **If UPS fails**.

Setting	Definition
Output Voltage	Defines the nominal AC voltage level for the UPS output.
Vout Reporting	Defines how the UPS scales its output voltage readings.
Output Frequency Range	Defines the nominal value for the frequency used by the output voltage.
If UPS fails	Defines how the UPS will respond if it cannot continue to provide output power, and frequency or voltage is out of range.

Alarm Thresholds (Symmetra UPS or Symmetra PX UPS)

The following table describes the **Alarm Thresholds** settings for the Symmetra UPS or Symmetra PX UPS.

Threshold	Definition
Alarm if Redundancy Under	Defines the redundancy below which an alarm occurs.
Alarm if Load Over	Defines the maximum equipment load that the UPS will support without generating an alarm.
Alarm If Runtime Under	Defines the amount of runtime below which an alarm occurs.

Shutdown Parameters

All of the following settings are available with Smart-UPS, Matrix-UPS, Symmetra UPS, and Symmetra PX UPS models. A Silcon UPS uses only the **Low-Battery Duration**, **Maximum Shutdown Time**, and **Shutdown Delay** settings (under **Shutdown Behavior Settings**).

In the control console, use the **Battery** option in the **Configuration** menu to access the **Return Battery Capacity** setting.

Action	Definition
Return Battery Capacity	Defines the minimum battery capacity required before the UPS turns on after a shutdown that was caused by a power failure. **NOTE:** The UPS must also wait the time defined by the **Return Delay** setting before it can turn on.
Low-Battery Duration	Defines how long the UPS can continue to run on battery power after a low-battery condition occurs. **NOTE:** This setting also defines the time available for PowerChute to safely shut down its server in response to the **Control** menu options **Turn UPS Off Gracefully**, **Reboot UPS Gracefully**, and **Put UPS To Sleep Gracefully**.
Maximum Shutdown Time (Web interface only)	Reports the delay that is defined by the **Maximum Shutdown Time** setting for the PowerChute Network Shutdown feature. **NOTE:** For information about the PowerChute Network Shutdown feature, see PowerChute (UPS PowerChute Network Shutdown); for information about how the **Maximum Shutdown Time** is determined, see Maximum-Shutdown-Time negotiation.
Shutdown Delay	Defines how long the UPS waits before it shuts down in response to a turn-off command.

Action	Definition
Return Delay	Defines how long the UPS waits before it turns on after a shutdown that was caused by a power failure. **NOTE:** The UPS must also have the capacity specified by the **Return Battery Capacity** setting before it can turn on.
Sleep Time	Defines how long the UPS sleeps (keeps its output power turned off) when you use either of the **Control** menu's sleep options (**Put UPS To Sleep** or **Put UPS To Sleep Gracefully**). **NOTE:** This setting also is in the "Control" page of the Web interface.

General Settings

Four **General Settings** are available for Smart-UPS. The first two settings (**UPS Name** and **Last Battery Replacement**) are available for all other UPS models.

Note

In the control console, use the **Battery** option in the **Configuration** menu to access the **Last Battery Replacement** and **External Batteries** settings.

Setting	Definition
UPS Name	Defines the name of the UPS.
Last Battery Replacement	Defines the date of the most recent UPS battery replacement. **NOTE:** Use *mm/dd/yy* format.
Self-Test Schedule (control console only)	Schedules when and how frequently a UPS self-test occurs. See Scheduled UPS self-tests.
Audible Alarm	Defines when Smart-UPS generates an alarm in response to switching to battery operation.
External Batteries	Defines how many external battery packs are connected to Smart-UPS XL. **NOTE:** Smart-UPS XL models cannot automatically sense and report the number of connected battery packs.
Simple Signal Shutdowns	When enabled, allows simple-signalling shutdown through PowerChute Network Shutdown

Reset UPS Defaults

This option resets the UPS to use the default EEPROM values.

Before you use this option, make sure that resetting the EEPROM values will not adversely affect the load equipment or any shutdown sequence.

Configure Parallel UPS parameters (Silcon UPS only)

Use this option, available only in the Web interface, to identify up to nine different Silcon UPSs that you can then access through the hyperlink, **View the refreshing status page**, in the "Status for UPS" page.

Setting	Definition
IP Address	Identifies the IP address of the Management Card of the Silcon UPS to be monitored.
Monitor Name	Identifies by name the Silcon UPS to be monitored.

Module Status (Symmetra UPS or Symmetra PX UPS)

Menu options

Symmetra UPS models have a **Module Status** option in the Web interface that provides status information about the modules used at that UPS.

Symmetra UPS and Symmetra PX UPS models have the following options in the UPS menu of the control console:

- **Module Diagnostics & Information** provides module status.
- **Raw Status Data** provides diagnostic information about the modules. APC engineers and customer support technicians use these data to troubleshoot hardware problems

Module status

Module status is reported for the following modules:

- The Intelligence Module
- The Redundant Intelligence Module
- The Power Modules
- The Battery in the Main Frame
- Any External Battery Frame
- Communication Bus (Symmetra PX UPS only)

For information about how to access a list of the UPS events, including the module-related, Symmetra status events, see “Event List” page.

PowerChute (UPS PowerChute Network Shutdown)

Overview

The **PowerChute** option of the UPS menu in the Web interface allows you to use the APC PowerChute Network Shutdown utility to shut down as many as 50 servers on your network that are using any client version of PowerChute Network Shutdown.

For more information about PowerChute Network Shutdown, see the *PowerChute Network Shutdown Installation Guide* (Install.htm) and the *PowerChute Network Shutdown Release Notes* (Relnotes.htm), provided in the **.\pcns** directory on the APC Network Management Card *utility* CD. Also, see the three flow diagrams provided in the CD's **.\trouble** directory: **PCNS Shutdown Behavior.pdf**, **PCNS Low-Battery Shutdown Behavior.pdf**, and **PCNS Maximum Shutdown Time Negotiation.pdf**.

PowerChute Network Shutdown Parameters

Parameter	Definition
Maximum Shutdown Time	Defines the maximum time that the UPS at a PowerChute Network Shutdown client waits before it shuts down in response to a graceful turn-off command. **NOTE:** For information about this shutdown delay is determined, see Maximum-Shutdown-Time negotiation.
Shutdown Behavior	Defines how the UPS turns off after the PowerChute Network Shutdown clients finish shutting down their computer systems.
Add Client IP Address	Allows you to add as many as 50 PowerChute Network Shutdown clients to the list **Configured Client IP Addresses**. **NOTE:** When you install a PowerChute Network Shutdown client on your network, it is added to the list automatically.
Configured Client IP Addresses	Allows you to view the list of PowerChute Network Shutdown clients, and remove PowerChute Network Shutdown clients from the list. **NOTE:** When you uninstall a PowerChute Network Shutdown client, it is removed from the list automatically.

Maximum-Shutdown-Time negotiation

The **Maximum Shutdown Time** setting provides the delay needed to make sure that a server has enough time to shut down safely when the Management Card or PowerChute Network Shutdown client initiates a graceful shutdown at that server.

For information about the **Turn UPS Off Gracefully**, **Reboot UPS Gracefully**, and **Put UPS To Sleep Gracefully** options that use this delay, see Control.

The time reported by the **Maximum Shutdown Time** setting represents the maximum delay needed by at least one of the servers listed in the **Configured Client IP Addresses** list. This time is determined by a negotiation process that is initiated when any of the following occurs:

- The Management Card turns on (a **System: Coldstart** event)
- The Management Card is reset (a **System: Warmstart** event)
- You select **Force negotiation** from the **Maximum Shutdown Time** setting's drop-down menu, and click **Apply**

During the negotiation process, which can take up to 10 minutes, each server listed in **Configured Client IP Addresses** is contacted to determine the shutdown delay needed by that server. The delay time defined by the **Maximum Shutdown Time** setting will be changed, if necessary, to the highest delay time reported by the servers.

For example:

- If **3 minutes** was the result of the last negotiation process, and a new server that requires a 4-minute shutdown delay has been added to the **Configured Client IP Addresses** list, **4 minutes** will be the new **Maximum Shutdown Time**.
- If none of the servers needs more than a 2-minute delay, **2 minutes** will be the **Maximum Shutdown Time** setting.

At the end of the negotiation process. two minutes time period is added to the calculated total for **Maximum Shutdown Time** to allow for any unusual delays that might occur in notifying servers to shut down.

For a flowchart of the negotiation process, see the **PCNS Maximum Shutdown Time Negotiation.pdf** file provided in the **.\trouble** directory on the APC Network Management Card *utility* CD. The **.\trouble** directory also has two other flowchart presentations about PowerChute Network Shutdown: **PCNS Shutdown Behavior.pdf** and **PCNS Low-Battery Shutdown Behavior.pdf**.

Scheduling (UPS Shutdown)

Overview

You can schedule shutdowns on a daily, weekly or one-time basis, and you can schedule them for a single UPS or for all UPSs in a Synchronized Control Group.

For more information about how to use this option, see the following sections:

- Examples
- How to schedule a shutdown
- How to schedule a synchronized shutdown
- How to edit, disable, or delete a shutdown

Examples

The following web page provides examples of **Daily**, **Weekly**, and **One-Time** shutdowns that were scheduled using the **Scheduling** option, which is available in the Web interface only.

How to schedule a shutdown

Click the **Daily**, **Weekly**, or **One-Time** option to choose the type of shutdown, and then use the following fields:

1. Use **Name of Scheduled Shutdown** to define a name for the shutdown.
2. Use **Shutdown** to define when the shutdown will begin.
3. Use **Turn back on** to define whether the UPS will turn on at a specific day and time, **Never** (the UPS will be turned on manually), or **Immediately** (the UPS will turn on after a six-minute delay).
4. Select whether PowerChute servers will be warned before the shutdown begins.
5. Click **Apply**.

How to schedule a synchronized shutdown

To use the Network Management Card's Web interface to schedule shutdowns within a Synchronized Control Group, always schedule all shutdowns through the same member of the group.

The following guidelines apply to Synchronized Control Groups:

- All UPSs in a Synchronized Control Group must be the same model.
- Synchronized Control Groups are supported for most UPS models of the Smart-UPS and Symmetra UPS product lines. Any Smart-UPS or Symmetra UPS with a card slot that accepts a Network Management Card supports Synchronized Control Groups.
- In a Synchronized Control Group of Symmetra 3-phase UPSs, the shutdown mode setting must be either normal or secure for each UPS.

Scheduled shutdowns through more than one group member is **not** a supported configuration and may cause unpredictable results.

All scheduled shutdowns will be synchronized when the Network Management Card that initiates the shutdown is a member of a Synchronized Control Group and its status as a group member is enabled.

How to edit, disable, or delete a shutdown

Click a listed shutdown to display the "Daily Shutdown Detail" page. Use this page to do the following:

- View a summary of the shutdown, including information about the values for settings that can affect how the UPS shuts down and turns on again:
  - For information about **Maximum Shutdown Time**, a **PowerChute** option setting, see Maximum-Shutdown-Time negotiation
  - For information about **Shutdown Delay** and **Return Delay**, see Shutdown Parameters
- Change any shutdown parameter.
- Use **Status of Scheduled Shutdown** to enable, disable or delete the shutdown.

Sync Control

Overview

The **Sync Control** option of the UPS menu displays the status of each member of the Synchronized Control Group, if any, in which this Management Card is a member and the parameters necessary for this Management Card to be identified and operate as a member of the group.

The following guidelines apply to Synchronized Control Groups:

- All UPSs in a Synchronized Control Group must be the same model.
- Synchronized Control Groups are supported for most UPS models of the Smart-UPS and Symmetra UPS product lines. Any Smart-UPS or Symmetra UPS with a card slot that accepts a Network Management Card supports Synchronized Control Groups.
- In a Synchronized Control Group of Symmetra 3-phase UPSs, the shutdown mode setting must be either normal or secure for each UPS.

Sync Control Group Status

Item	Description
IP Address	The IP address of the group member
Input Status	The state of the group member's input power: **good** (acceptable) or **bad** (not acceptable)
Output Status	The status of the group members output power: **On** or **Off**.

Configure Synchronized Control

Parameter	Description
Synchronized Group Membership	Determines whether this Synchronized Control Group member is an active member of its group. If you set this value to **Disabled** (the default value), the Management Card ignores all Synchronized Control Group commands, and its UPS functions as if it were not a member of any Synchronized Control Group.
Synchronized Control Group Number	The unique identifier of the Synchronized Control Group of which this Management Card's UPS is a member. This value must be a number from 1 through 65534. A UPS can be a member of only one Synchronized Control Group. All members of a Synchronized Control Group must have the same **Synchronized Control Group Number** and **Multicast IP Address**.
Power Synchronized Delay	The maximum time (120 seconds by default) that the initiating UPS of a synchronized sleep or reboot action will wait for other group members to regain input power when the initiating UPS is ready to turn on. • For a synchronized reboot, the initiating UPS waits up to this delay period for other group members to regain input power, then waits until its return battery capacity is reached, and then begins the **Return Delay**. The **Power Synchronized Delay** does not occur if all group members have input power immediately after they turn off for the reboot. • For a synchronized sleep command, after the configured sleep time expires, the initiating UPS waits up to this delay period for other group members to regain input power, and then begins the **Return Delay**. The **Power Synchronized Delay** does not occur if all group members have input power after the sleep time expires.
Return Battery Capacity Offset	An amount of battery capacity, as a percentage, that is configured individually for each member of the Synchronized Control Group. This offset percentage allows you to set a different and lower **Return Battery Capacity** for each group member for use during synchronized actions only. To determine the **Return Battery Capacity** that will be required of each participating group member during a synchronized **Turn UPS On**, **Reboot UPS**, **Reboot UPS Gracefully**, **Sleep**, or **Sleep Gracefully** action, this offset percentage is subtracted from the **Return Battery Capacity** of the UPS that initiates the action.

Parameter	Description
Multicast IP Address	The IP address used by members of a Synchronized Control Group to communicate with each other. This address must be within the range of 224.0.0.3 to 224.0.0.254. All members of the Synchronized Control Group must have the same group number and multicast IP address.

Environment Menu

Introduction

Overview

Use the **Environment** menu in the Web interface or control console to manage an external environmental monitor or the Integrated Environmental Monitor of an AP9618 or AP9619 Network Management Card. (In the control console, the **Environment** menu is an option of the **Device Manager** menu.)

- When you select the **Environment** option in an AP9617 Network Management Card's control console, you access the menu options used to manage an external environmental monitoring device.
- When you select the **Environment** option in an AP9618 Network Management Card's control console, two options may be available:

```
1- Integrated Environmental Monitor Settings
2- External Environmental Monitor Settings
```

Environment menu options

Two basic types of options are available:

- Status Options
- Settings Options

Each of the control console's **Environmental Monitor Settings** menus has an **About Environmental Monitor** option that accesses firmware information for these environmental monitors; the Web interface provides this firmware information in the "Environmental Monitor Status" page.

Status Options

Overview

The “Summary Page” of the Web interface displays basic status information about the environmental monitor thresholds and contacts and about the Integrated Environmental Monitor’s output relay at an AP9618 or AP9619 Network Management Card. Use the **Status** option in the **Environment** menu to access detailed status about these environmental monitor components, including how the current humidity and temperature readings relate to their high and low thresholds.

The Web interface uses icons to identify faults that exist at an environmental monitor. For information about these status icons, see Quick status tab.

In the control console, basic status information is displayed above the **Control Console** and **Environmental Monitor Settings** menus. Use **Threshold and Contact Details** (in the **External Environmental Monitor Settings** menu) and **Detailed Status** (in the **Integrated Environmental Monitor Settings** menu) for detailed status of the environmental monitor components.

Probe status

The Web interface uses Temperature and Humidity graphs to identify whether the reported value exceeds a low (blue) or high (red) threshold for each of the identified probes:

- Up to two probes at an AP9617 Network Management Card
- Up to three probes at an AP9618 or AP9619, Network Management Card with the Integrated Environmental Monitor probe listed last

In the control console, the status options in the **Environmental Monitor Settings** menus report the high and low thresholds for the specific environmental monitor's probes and any violations of those thresholds.

Contact status

The Web interface reports the current state (**Disabled**, **No Fault**, or **Fault Present**) for each identified input contact:

- Up to four contacts for an external environmental monitor
- Two contacts for the Integrated Environmental Monitor at an AP9618 or AP9619 Network Management Card.

In the control console, the status options in the **Environmental Monitor Settings** menus reports the current fault condition for each of the specific environmental monitoring's contacts.

Output relay status (AP9618 or AP9619)

The Web interface reports the current state of the Integrated Environmental Monitor's output relay at an AP9618 or AP9619 Network Management Card

In the control console, the **Output Relay** option in the Integrated Environmental Monitor menu reports the current condition.

Settings Options

Probe settings

In the Web interface, use the **Probes** option in the **Environment** menu to access the following fields:

- **Setting** fields that define a name (16-character maximum) and high and low temperature and humidity thresholds, for each probe
- **Event Generation** fields that enable or disable the generation of an event when a selected threshold violation occurs.

In the control console, use the **Probe Settings** option in the **Environmental Monitor Settings** menus to define the probe name, temperature and humidity thresholds, and event generation settings.

Contact settings

In the Web interface, use the **Input Contacts** option in the **Environment** menu to access the following fields:

- **Name** fields to define the name for each contact alarm (16-character maximum)
- **Event Generation** fields to enable or disable each alarm.

In the control console, use the **Contact Settings** options in the **Environmental Monitor Settings** menu to access these settings.

Output relay settings (AP9618 or AP9619)

To access the following settings:

- In the Web interface, use the **Output Relay** option in the **Environment** menu.
- In the control console, use the **Output Relay Settings** option in the **Integrated Environmental Monitor** menu.

Setting	Definition
Output Relay (Web interface) Relay Name (control console	Defines a description of the output relay's purpose (16-character maximum).
Switch When (Web interface Switch Relay When (control console)	Selects the event that will activate the output relay (or disables the action).
Delay (Web interface) Switch to Relay Delay (control console)	Defines how long in seconds the event that is selected to activate the output relay must be present before the output relay is activated.
Hold (Web Interface) Relay Hold Time (control console)	Defines the minimum number of seconds that the output relay will remain activated after its activating event occurs.

Event-Related Menus

Introduction

Overview

Use the options of the **Events** menu to do the following tasks:

- Access the Event Log.
- Define the actions to be taken when an event occurs, based on the severity level of that event. (You must use the Web interface to define which events will use which actions.)
  - Event logging
  - Syslog messages
  - SNMP trap notification
  - E-mail notification

To define which events will use which actions, see Event Log and How to Configure Individual Events.

- Define up to four SNMP trap receivers, by NMS-specific IP address, for event notifications by SNMP traps.
- Define up to four recipients for event notifications by e-mail.

Menu options

To access the event-related options:

- In the Web interface, use the **Events** menu.
- In the control console:
  - Use the **Email** option in the **Network** menu to define the SMTP server and e-mail recipients
  - Use the **SNMP** option in the **Network** menu to define the SNMP trap receivers
  - Use CTRL-L to access the event log from any menu

For information about event-related settings and about the e-mail feature, see the following descriptions:

- Event Log
- Event Actions (Web Interface Only)
- Event Recipients
- E-mail Feature
- How to Configure Individual Events

Event Log

Overview

The Management Card supports event logging for all UPS application firmware modules. You can record and view UPS, environmental monitor, and Management Card events.

Use any of the following to view the Event Log:

- Web interface
- Control console
- FTP
- SCP

Logged events

By default, the following events are logged:

- Any event that causes an SNMP trap, except for SNMP authentication failures.
- The Management Card's abnormal internal system events

To disable the logging of events based on their assigned severity level, use the **Actions** option in the Web interface's **Events** menu.

See Event Actions (Web Interface Only).

Even if you disable the Event Log for all severity levels, some System (Management Card) events will still be logged because some of those events have no severity level.

To access a list of the UPS and Management Card events, see "Event List" page.

The Event Log will log a graceful shutdown of the UPS, even when that shutdown was not initiated by the Management Card

- A graceful shutdown from Serial Port 1 typically indicates that PowerChute or PowerNet Manager performed the shutdown
- A graceful shutdown from Serial Port 0 typically indicates that a management peripheral, such as the Out-of-Band Management Card, initiated the shutdown.

Web interface

The **Log** option in the **Events** menu accesses the event log, which displays all of the events that have been recorded since the log was last deleted, in reverse chronological order. The **Delete Log** button clears all events from the log.

Control console

In the control console, press CTRL-L to display up to 300 events from the event log, in reverse chronological order. Use the SPACE BAR to scroll through the recorded events.

While viewing the log, type `d` and press ENTER to clear all events from the log.

Deleted events cannot be retrieved.

How to use FTP or SCP to retrieve log files

If you are an Administrator or Device Manager, you can use FTP or SCP to retrieve a tab-delineated event log file (*event.txt*) or data log file (*data.txt*) that you can import into a spreadsheet application.

- The file reports all of the events or data recorded since the log was last deleted.
- The file includes information that the event log or data log does not display.
  - The version of the file format (first field)
  - The date and time the file was retrieved
  - The **Name**, **Contact**, and **Location** values and IP address of the Management Card
  - The unique **Event Code** for each recorded event (*event.txt* file only)

The Management Card uses a four-digit year for log entries. You may need to select a four-digit date format in your spreadsheet application to display all four digits of the year.

If you are using the encryption-based security protocols for your system, use Secure CoPy (SCP) to retrieve the log file. (You should have FTP disabled.)

If you are using unencrypted authentication methods for the security of your system, use FTP to retrieve the log file.

See Security for information on the available protocols and methods for setting up the type of security appropriate for your needs.

To use SCP to retrieve the files. To use SCP to retrieve the *event.txt* file, use the following command:

```
scp username@hosthame_or_ip_address:event txt ./event.txt
```

To use SCP to retrieve the *data.txt* file, use the following command:

```
scp username@hosthame_or_ip_address:data.txt ./data.txt
```

To use FTP to retrieve the files. To use FTP to retrieve the *event.txt* or *data.txt* file:

1. At a command prompt, type `ftp` and the Management Card's IP address, and press ENTER.

   If the **Port** setting for **FTP Server** in the **Network** menu has changed from its default value (**21**), you must use the non-default value in the FTP command. For Windows FTP clients, use the following command, including spaces. (For some FTP clients, you must use a colon instead of a space between the IP address and the port number.)

   ```
   ftp>open ip_address port_number
   ```

   To use non-default port values to enhance security, see Port assignments.

2. Use the case-sensitive **User Name** and **Password** for either an Administrator or a Device Manager user to log on.
   - For Administrator, **apc** is the default for **User Name** and **Password**.
   - For Device Manager, **device** is the default for **User Name**, and **apc** is the default for **Password**.
3. Use the **get** command to transmit the text-version of the event log or data log to your local drive.

   ```
   ftp>get event.txt
   ```

   or

   ```
   ftp>get data.txt
   ```

4. You can use the **del** command to clear the contents of the event log or data log.

   ```
   ftp>del event.txt
   ```

   or

   ```
   ftp>del data.txt
   ```

   You will not be asked to confirm the deletion.
   - If you clear the data log, the event log records a deleted-log event.
   - If you clear the event log, a new *event.txt* file is created to record the deleted-log event.
5. Type `quit` at the `ftp>` prompt to exit from FTP.

Event Actions (Web Interface Only)

Overview

Use the **Actions** option in the **Events** menu to do the following:

- Select which actions will occur for events that have a severity level:
  - **Event Log** selects which severity levels cause an event to be recorded in the event log.

     See Event Log action.

  - **Syslog** selects which severity levels cause messages to be sent to Syslog servers to log events.

     See Syslog action.

  - **SNMP Traps** selects which severity levels cause SNMP traps to be generated.

     See SNMP Traps action.

  - **Email** selects which severity levels cause e-mail notifications.

     See Email action.

- Click **Details** for a complete list of the Management Card (System), UPS, and environmental monitor (Environment) events that can occur, and then edit the actions that will occur for an individual event.

   See How to Configure Individual Events.

- Click **Hide Details** to return to the **Actions** option.

Severity levels

Except for some system (Management Card) events that do not have a severity level, events are assigned a default severity level.

- **Informational**: Indicates an event that requires no action, such as a notification of a return from an abnormal condition.
- **Warning**: Indicates an event that may need to be addressed if the condition continues, but which does not require immediate attention.
- **Severe**: Indicates an event that requires immediate attention.
  - Unless resolved, severe UPS and Management Card events can cause incorrect operation of the UPS or its supported equipment, or can result in the loss of UPS protection during a power failure.
  - Severe Environmental monitoring device events warn of abnormal environmental conditions or possible security violations.

Event Log action

To stop logging events that have a severity level, disable the **Event Log** action. System (Management Card) events that have no severity level will still be logged. By default, all events are logged, even events that have no severity level.

For more information about the log, see Event Log.

Syslog action

By default, the **Syslog** action is enabled for all events that have a severity level. However, before you can use this feature to send Syslog messages when events occur, you must configure it.

See Syslog.

SNMP Traps action

By default, the **SNMP Traps** action is enabled for all events that have a severity level. However, before you can use SNMP traps for event notifications, you must identify the NMSs (by their IP addresses) that will receive the traps.

To define up to four NMSs as trap receivers, see Event Recipients.

Email action

By default, the **Email** action is enabled for all events that have a severity level. However, before you can use e-mail for event notifications, you must define the e-mail recipients.

See E-mail Feature.

Event Recipients

Overview

You can use the Web interface or control console to define the trap receivers and up to four e-mail addresses to be used when an event occurs that has SNMP traps or e-mail enabled, as described in Event Actions (Web Interface Only).

To identify the servers that will receive Syslog messages, see Syslog.

Trap Receivers

To define the **Trap Receiver** settings that determine which NMSs will receive traps:

- In the Web interface, use the **Recipients** option in the **Events** menu.
- In the control console, use the **SNMP** option in the **Network** menu.

Item	Definition
Community Name	The password (maximum of 15 characters) used when traps are sent to the NMS identified by the **Receiver NMS IP** setting.
Receiver NMS IP	The IP address of the NMS that will receive traps. If this setting is **0.0.0.0** (the default value), traps will not be sent to any NMS.
Generation (Web Interface) Trap Generation (control console)	Enables (by default) or disables the sending of any traps to the NMS identified by the **Receiver NMS IP** setting.
Authentication Traps	Enables or disables the sending of authentication traps to the NMS identified by the **Receiver NMS IP** setting.

Email options

See E-mail Feature.

E-mail Feature

Overview

Use the Simple Mail Transfer Protocol (SMTP) to send e-mail to up to four recipients when an event occurs.

To use the e-mail feature, you must define the following settings:

- The IP addresses of the primary and secondary Domain Name Service (DNS) servers

See DNS servers.

- The DNS name of the **SMTP Server** and the **From Address** settings for SMTP

See SMTP settings.

- The e-mail addresses for a maximum of four recipients

See Email Recipients.

Note

You can use the **To Address** setting of the **Email Recipients** option to send e-mail to a text-based pager.

DNS servers

The Management Card cannot send any e-mail messages unless at least the IP address of the primary DNS server is defined.

See DNS.

The Management Card will wait a maximum of 15 seconds for a response from the primary DNS server or the secondary DNS server (if a secondary DNS server is specified). If the Management Card does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers that are on the same segment as the Management Card, or on a nearby segment (but not across a wide-area network (WAN).

After you define the IP addresses of the DNS servers, verify that DNS is working correctly by entering the DNS name of a computer on your network to look up the IP address for computer.

SMTP settings

Use the **Email** option in the **Network** menu to define the following settings:

Setting	Description
SMTP Server	The DNS name of the SMTP server. **NOTE:** This definition is required only when the **SMTP Server** option is set to **Local**. See Email Recipients.
From Address	The contents of the **From** field in the e-mail messages sent by the Management Card. **NOTE:** The SMTP server's configuration may require that you use a valid user account on the server for this setting. See the server's documentation for more information.

Email Recipients

In the Web interface, use the **Recipients** option in the **Events** menu or the **Configure the Email recipients** link in the “Email Configuration” page to identify up to four e-mail recipients. Use the **Email Test** option to send a test message to a configured recipient.

In the control console, use the **Email** option in the **Network** Menu, to access the e-mail recipient settings.

Setting	Description
To Address†	Defines the user and domain names of the recipient. To use e-mail for paging, use the e-mail address for that recipient's pager gateway account (for example, `myacct100@skytel.com`). The pager gateway will generate the page. **NOTE:** The recipient's pager must be able to use text-based messaging.
Use SMTP Server	Selects one of the following methods for routing e-mail: • Through the Management Card's SMTP server (the recommended option, **Local**. This option ensures that the e-mail is sent before the Management Card's 20-second time-out, and, if necessary, is retried several times. Also do one of the following: •Enable forwarding at the Management Card's SMTP server so that it can route e-mail to external SMTP servers. Typically, SMTP servers are not configured to forward e-mail. Always check with the administrator of your SMTP server before changing its configuration to allow forwarding. •Set up a special e-mail account for the Management Card to forward e-mail to an external mail account. • Directly to the recipient's SMTP server (the **Recipient's** option). On a busy remote SMTP server, the time-out may prevent some e-mail from being sent, and with this option the Management Card tries to send the e-mail only once. When the recipient uses the Management Card's SMTP server, this setting has no affect.
Generation	Enables (by default) or disables sending e-mail to the recipient.

† You can bypass the DNS lookup of the mail server's IP address by using the IP address in brackets instead of the e-mail domain name. For example, use jsmith@[xxx,xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly.

Setting	Description
Format	Selects the format used for e-mail messages: **Short**: Identifies only the event that occurred. For example: UPS: Communications Established **Long**: Includes information about the Management Card and the UPS, as well as the event. For example: Name : Test Lab Location : Building 3 Contact : Don Adams http://139.225.6.133 Serial # : Wa12 UPS Ser # : XS9849007541 Date: 06/12/2003 Time: 16:09:48 Code: 0x0002 Severe - UPS: Communications Established

† You can bypass the DNS lookup of the mail server's IP address by using the IP address in brackets instead of the e-mail domain name. For example, use jsmith@[xxx,xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly.

How to Configure Individual Events

"Event List" page

The **Actions** option in the **Events** menu opens the "Event Actions Configuration" page. Use the **Details** button in this page for a complete list of the Management Card (System), UPS, and environmental monitor (Environment) events that can be reported by your Management Card.

Each event is identified by its unique code, its description, and its assigned severity level, as shown in the following examples.

For information about severity levels and how they define the actions associated with events, see Event Actions (Web Interface Only).

Code	Description	Severity
0x0008	System: Password changed.	Informational
0x0109	UPS: Switched to battery backup power.	Warning
0x030F	Environment: High humidity threshold violation on probe 1.	Severe

"Detailed Event Action Configuration" page

The event codes provide a link to a page that allows you to do the following:

- Change the selected event's severity level
- Enable or disable whether the event uses the Event Log, Syslog messages, SNMP traps, or e-mail notifications

Data Menu (Web Interface Only)

Log Option

Use this option to access a log that stores information about the UPS, the power input to that UPS, and the ambient temperature and relative humidity measured by an environmental monitor's probes.

Use the **Data** menu's **Configuration** option to define how frequently data is sampled and stored in the data log. Each entry is listed by the date and time the data was recorded, and provides the data in a column format.

The data recorded depends on the UPS model.

See Configuration Option.

For descriptions of the recorded data that is specific to your UPS, see the online help in your Management Card's Web interface.

To retrieve the data log as a text file, see How to use FTP or SCP to retrieve log files.

Configuration Option

Use this option to access the “Data Log Configuration” page. which reports how much data can be stored in the data log. If you change the **Log Interval** setting, which defines how often data will be sampled and recorded in the data log, the report updates based on the new setting.

The minimum interval is **60** seconds; the maximum interval is **8** hours, **10** minutes, **15** seconds.

Boot Mode

Introduction

Overview

In addition to using a BOOTP server or manual settings, the Network Management Card can use a dynamic host configuration protocol (DHCP) server to provide the settings the Management Card needs to operate on a TCP/IP network.

To use a DHCP server to provide the Management Card's network settings, use **Boot mode**, a **TCP/IP** option in the **Network** menu. **Boot mode** must be set to either **DHCP & BOOTP**, its default setting, or **DHCP only**.

For information on DHCP and DHCP options, see RFC2131 and RFC2132.

DHCP & BOOTP boot process

When **Boot mode** is set to its default **DHCP & BOOTP** setting, the following occurs when the Management Card is turned on or reset:

1. The Management Card makes up to five requests for its network assignment from any BOOTP server. If a valid BOOTP response is received, the Management Card starts the network services and sets **Boot mode** to **BOOTP Only**.
2. If the Management Card fails to receive a valid BOOTP response after five BOOTP requests, the Management Card makes up to five requests for its network assignment from any DHCP server. If a valid DHCP response is received, the Management Card starts the network services and sets **Boot mode** to **DHCP Only**.

   Note

   To configure the Management Card so that it always uses the **DHCP & BOOTP** setting for **Boot mode**, enable the option **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**, which is disabled by default.

   See Management Card settings.
3. If the Management Card fails to receive a valid DHCP response after five DHCP requests, it repeats sending BOOTP and DHCP requests until it receives a valid network assignment: first it sends a BOOTP request every 32 seconds for 12 minutes, then it sends one DHCP request with a time-out of 64 seconds, and so forth.


Note

If a DHCP server responds with an invalid offer (for example, the offer does not contain the APC Cookie), the Management Card accepts the lease from that server on the last request of the sequence and then immediately releases that lease. This prevents the DHCP server from reserving the IP Address associated with its invalid offer.

For more information on what a valid response requires, see DHCP response options.

DHCP Configuration Settings

Management Card settings

Use the **TCP/IP** option in the **Network** menu of either the Web interface or the control console to configure the network settings of the Management Card.

- The **Port Speed**, **Host Name**, and **Domain Name** settings are available for any **Boot mode** selection
- The **Vendor Class**, **Client ID**, and **User Class** settings are available for any **Boot mode** selection except **Manual**.

See Advanced settings.

When **Boot mode** is set to **DHCP & BOOTP**, two options are available:

- **After IP Assignment** in the control console (or **Remain in DHCP & BOOTP mode after accepting TCP/IP settings** in the Web interface): By default, this option switches **Boot mode** to the selection based on the server that provided the TCP/IP settings (**DHCP Only** or **BOOTP Only**).
- **DHCP Cookie Is** in the control console (or **Require vendor specific cookie to accept DHCP Address** in the Web interface): By default, this option requires that the DHCP responses include the APC cookie in order to be valid.

For more information about the APC cookie, see DHCP response options.

When **Boot mode** is set to **DHCP Only**. two options are available:

- **DHCP Cookie Is** in the control console (or **Require vendor specific cookie to accept DHCP Address** in the Web interface): By default, this option requires that the DHCP responses include the APC cookie in order to be valid.
- **Retry Then Stop** in the control console (**Maximum # of Retries** in the Web interface), This option sets the number of times the Management Card will repeat the DHCP request if it does not receive a valid response. The default setting (**0** in the Web interface, **None** in the control console), requires that the Management Card continuously send out DHCP requests until a valid DHCP response is received.

DHCP response options

Each valid DHCP response contains options that provide the TCP/IP settings a Management Card needs to operate on a network and other information that affects the Management Card's operation.

A Management Card uses the Vendor Specific Information option (option 43) in a DHCP response to determine whether the DHCP response is valid.

Vendor Specific Information (option 43). The Vendor Specific Information option contains up to two APC-specific options encapsulated in a TAG/LEN/DATA format: the APC Cookie and the Boot Mode Transition.

APC Cookie. Tag 1, Len 4, Data "1APC"

Option 43 communicates to the Management Card that a DHCP server has been configured to service APC devices. By default, the APC Cookie must be present in this DHCP response option before a Management Card can accept the lease.

To disable the requirement of an APC cookie, see Management Card settings for information on the **DHCP Cookie Is** setting.

Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie:

```
Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43
```

Boot Mode Transition. Tag 2, Len 1, Data 1/2

This option 43 setting enables or disables the **After IP Assignment** option which, by default, causes the **Boot mode** option to base its setting on the server that provided the network assignment values (**DHCP Only** or **BOOTP Only**):

- A data value of 1 disables the **After IP Assignment** option. The **Boot mode** option remains as **DHCP & BOOTP** after network values are assigned successfully. Whenever the Management Card reboots, it will request its network assignment first from a BOOTP server, and then, if necessary, from a DHCP server.

  
  See DHCP & BOOTP boot process.

- A data value of 2 enables the **After IP Assignment** option. The **Boot mode** option switches to **DHCP Only** when the Management Card accepts the DHCP response. Whenever the Management Card reboots, it will request its network assignment from a DHCP server, only.

  
  For more information about the **After IP Assignment** option, see Management Card settings.

Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie and the disable Boot Mode Transition setting:

```
Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43 0x02 0x01 0x01
```

TCP/IP options. A Management Card uses the following options within a valid DHCP response to define its TCP/IP settings:

- **IP Address** (from the **yiaddr** field of the DHCP response): The IP address that the DHCP server is leasing to the Management Card.
- **Subnet Mask** (option 1): The Subnet Mask value which the Management Card needs to operate on the network.
- **Default Gateway** (option 3): The default gateway address, which the Management Card needs to operate on the network.
- **Address Lease Time** (option 51): The time duration for the lease associated with the identified **IP Address.**
- **Renewal Time, T1** (option 58): The time that the Management Card must wait after an IP address lease is assigned before it can request a renewal of that lease.
- **Rebinding Time, T2** (option 59): The time that the Management Card must wait after an IP address lease is assigned before it can seek to rebind that lease.

Other options. A Management Card uses the following options within a valid DHCP response to define NTP, DNS, hostname and domain name settings:

- **NTP Server, Primary and Secondary** (option 42): Up to two NTP servers that can be used by the Management Card.
- **NTP Time Offset** (option 2): The offset of the Management Card's subnet, in seconds, from Coordinated Universal Time (UTC), formerly Greenwich Mean Time (GMT).
- **DNS Server, Primary and Secondary** (option 6):Up to two DNS servers that can be used by the Management Card.
- **Host Name** (option 12): The host name to be used by the Management Card (32-character maximum length).
- **Domain Name** (option 15): The domain name to be used by the Management Card (64-character maximum length).

Security

Security Features

Planning and implementing security features

As a network device that passes information across the network, the Network Management Card is subject to the same exposure as other devices on the network.

Use the information in this section to plan and implement the security features appropriate for your environment.

Summary of access methods

Serial control console.

Security Access	Description
Access is by user name and password.	Always enabled.

Remote control console.

Security Access	Description
Available methods: • User name and password • Selectable server port • Server Enable/Disable • Secure SHell (SSH)	For high security, use SSH. • With Telnet, the user name and password are transmitted as plain text. • SSH disables Telnet and provides encrypted access to the control console interface to provide additional protection from attempts to intercept, forge, or alter data during data transmission.

SNMP.

Security Access	Description
Available methods: • Community Name • NMS IP filters • Agent Enable/Disable • 4 access communities with read/write/disable capability	The NMS IP filters allow access from designated IP addresses. • 159.215.12.1 allows only the NMS with that IP address to have access. • 159.215.12.255 allows access for any NMS on the 159.215.12 segment. • 159.215.255.255 allows access for any NMS on the 159.215 segment. • 159.255.255.255 allows access for any NMS on the 159 segment. • 0.0.0.0 or 255.255.255.255 allows access for any NMS.

File transfer protocols.

Security Access	Description
Available methods: • User name and password • Selectable server port • Server Enable/Disable • Secure CoPy (SCP)	With FTP, the user name and password are transmitted as plain text, and files are transfered without the protection of encryption. Using SCP instead of FTP encrypts the user name and password and the files being transferred, such as firmware updates, configuration files, log files, Secure Socket Layer (SSL) certificates, and Secure SHell (SSH) host keys. If you choose SCP as your file transfer protocol, enable SSH and disable FTP.

Web Server.

Security Access	Description
Available methods: • User name and password • Selectable server port • Server Enable/Disable • MD5 authentication • Secure Socket Layer (SSL) and Transport Layer Security (TLS)	In basic HTTP authentication mode, the user name and password are transmitted base-64 encoded (with no encryption). MD5 authentication mode uses a user name and password phrase. SSL and TLS are available on Web browsers supported for the Network Management Card and on most Web servers. The Web protocol Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) encrypts and decrypts page requests to the Web server and pages returned by the Web server to the user.

Changing default user names and passwords immediately

As soon as you complete the installation and initial configuration of the Management Card, immediately change the default user names and passwords. Configuring unique user names and passwords is essential to establish basic security for your system.

Port assignments

If a Telnet, FTP, SSH/SCP or Web/SSL/TLS server uses a non-standard port, a user must specify the port when using the client interface, such as a Web browser. The non-standard port address becomes an extra "password," hiding the server to provide an additional level of security. The TCP ports for which these servers listen are initially set at the standard "well known ports" for the protocols. To hide the interfaces, use any port numbers from 5000 to 32768.

User names, passwords, community names (SNMP)

All user names, passwords, and community names for SNMP are transferred over the network as plain text. A user who is capable of monitoring the network traffic can determine the user names and passwords required to log in to the accounts of the control console or Web interface of the Network Management Card. If your network requires the higher security of the encryption-based options available for the control console and Web interface, be sure to disable SNMP access or set its access to read-only. (Read-only access allows you to receive status information and to use SNMP traps.)

Authentication

Authentication versus encryption

You can select to use security features for the Network Management Card that control access by providing basic authentication through user names, passwords, and IP addresses, without using encryption. These basic security features are sufficient for most environments in which sensitive data are not being transferred.

For a security method that provides additional authentication for the Web interface, but does not provide the higher security of encryption, use Message Digest 5 (MD5) Authentication.

See MD5 authentication (for the Web interface)

To ensure that data and communication between the Network Management Card and the client interfaces, such as the control console and the Web interface, cannot be intercepted, you can provide a greater level of security by using one or more of the following encryption-based methods:

- For the Web interface, use the Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols. You can also use these protocols in combination with MD5 authentication.
- To encrypt user names and passwords for control console access, use the Secure SHell (SSH) protocol.
- To encrypt user names, passwords, and data for the secure transfer of files, use the Secure CoPy (SCP) protocol.

For more information on these protocols for encryption-based security, see Secure SHell (SSH) and Secure CoPy (SCP) and Secure Socket Layer (SSL)/Transport Layer Security (TLS)

MD5 authentication (for the Web interface)

The Web interface option for MD5 authentication enables a higher level of access security than the basic HTTP authentication scheme. The MD5 scheme is similar to CHAP and PAP remote access protocols. Enabling MD5 implements the following security features:

- The Web server requests a user name and a password phrase (distinct from the password). The user name and password phrase are not transmitted over the network, as they are in basic authentication. Instead, a Java login applet combines the user name, password phrase, and a unique session challenge number to calculate an MD5 hash number. Only the hash number is returned to the server to verify that the user has the correct login information; MD5 authentication does not reveal the login information.
- In addition to the login authentication, each form post for configuration or control operations is authenticated with a unique challenge and hash response.
- After the authentication login, subsequent page access is restricted by IP addresses and a hidden session cookie. (You must have cookies enabled in your browser.) Pages are transmitted in their plain-text form, with no encryption.

If you use MD5 authentication for the Web interface, be sure to increase the security for other interfaces to the Management Card.

- **Control console:** Use SSH (which disables Telnet) for encrypted access.
- **File transfer:** Disable FTP, and instead use SCP, which encrypts user names, passwords, and files.
- **SNMP:** Disable SNMP or disable its write access. With read-only access, trap facilities remain available.

For additional information on MD5 authentication, see RFC document #1321 at **http://www.ietf.org**, the Web site of the Internet Engineering Task Force. For CHAP, see RFC document #1994.

You can use MD5 and the encryption-based SSL/TSL security protocols together. See Secure Socket Layer (SSL)/ Transport Layer Security (TLS) for an example of the extra security benefits of using both.

Encryption

Secure SHell (SSH) and Secure CoPy (SCP)

The Secure SHell (SSH) protocol provides a secure mechanism to access computer consoles or *shells* remotely. The protocol authenticates the server (in this case, the Network Management Card) and encrypts all transmissions between the SSH client and the server.

- SSH is an alternative to Telnet, which does not provide encryption.
- SSH protects the username and password, the credentials for authentication, from being used by anyone intercepting network traffic.
- To authenticate the SSH server (the Network Management Card) to the SSH client, SSH uses a host key that is unique to the SSH server and that provides an identification that cannot be falsified. Therefore, an invalid server on the network cannot obtain a user name and password from a user by presenting itself as a valid server.

To create a host key, see the *Management Card Addendum* (**.\doc\Addendum.pdf**) on the APC Network Management Card *utility* CD

- The Network Management Card supports versions 1 and 2 of SSH. The encryption mechanisms of the versions differ, and each version has advantages. Version 1 provides faster login to the Management Card, and version 2 provides improved protection from attempts to intercept, forge or change data that are transmitted.
- When you enable SSH, Telnet is automatically disabled.
- The interface, user accounts, and user access rights are the same whether you access the control console through SSH or Telnet.

For information on supported SSH client applications, see Telnet/SSH.

Secure CoPy (SCP) is a secure file transfer application that you can use instead of FTP. SCP uses the SSH protocol as the underlying transport protocol for encryption of user names, passwords, and files.

- When you enable and configure SSH, you automatically enable and configure SCP. No further configuration of SCP is needed.
- You must explicitly disable FTP. It is **not** disabled by enabling SSH.

Secure Socket Layer (SSL)/Transport Layer Security (TLS)

For secure Web communication, you enable Secure Socket Layer (SSL) and Transport Layer Security (TLS) by selecting HTTPS (SSL/TLS) as the protocol mode to use for access to the Web interface of the Network Management Card. Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is a Web protocol that encrypts and decrypts page requests from the user and pages that are returned by the web server to the user. Originally developed by Netscape, it has become an internet standard supported by most Web browsers.

The Network Management Card supports SSL version 3.0 and TLS version 1.0. Most browsers let you select the version of SSL to enable.

When SSL is enabled, your browser displays the lock icon, usually at the bottom of the screen.

SSL uses a digital certificate to enable the browser to authenticate the server (in this case, the Network Management Card). The browser verifies the following:

- The format of the server certificate is correct.
- The server certificate's expiration date and time has not passed.
- The DNS name or IP address specified when a user logs on matches the common name in the server certificate.
- The server certificate is signed by a trusted certifying authority.

Each major browser manufacturer distributes CA root certificates of the commercial Certificate Authorities in the certificate store (cache) of its browser so that it can compare the signature on the server certificate to the signature on a CA root certificate.

You can use the APC Security Wizard, provided on the APC Network Management Card *utility* CD, to create a certificate signing request to an

external Certificate Authority, or if you do not want to use an existing Certificate Authority, you can create an APC root certificate to upload to a browser's certificate store (cache). You can also use the Wizard to create a server certificate to upload to the Management Card.

See Creating and Installing Digital Certificates for a summary of how these certificates are used.

To create certificates and certificate requests, see the *Management Card Addendum* (**.\doc\Addendum.pdf**) on the APC Network Management Card utility CD

SSL also uses various algorithms and encryption ciphers to authenticate the server, encrypt data, and ensure the integrity of the data (i.e. that it has not been intercepted and sent by another server).

See CipherSuite to select which authentication and encryption algorithms to use.

You can use SSL/TLS and MD5 authentication together to provide the security benefits of both. MD5 authentication does not provide encryption, but its authentication methods can be a useful enhancement to the security provided by SSL/TLS.

Web browsers cache (save) Web pages that you recently accessed and allow you to return to those pages without re-entering your user name and password. MD5 authentication, however, requires you to enter your user name and password even to access a cached Web page, e.g., when you use the **Back** button of Microsoft Internet Explorer.

Therefore, if you are use the SSL and TLS protocols without also using MD5 authentication, always close your browser session before you leave your computer unattended.

Creating and Installing Digital Certificates

Purpose

For network communication that requires a higher level of security than password encryption, the Web interface of the Network Management Card supports the use of digital certificates with the Secure Socket Layer (SSL) protocol. Digital certificates can authenticate the Network Management Card (the server) to the Web browser (the SSL client).

The sections that follow summarize the three methods of creating, implementing, and using digital certificates. Read these sections to determine the most appropriate method for your system.

- Method 1: Use APC's default certificate.
- Method 2: Use the APC Security Wizard to create a CA certificate and a server certificate.
- Method 3: Use the APC Security Wizard to create a certificate-signing request to be signed by the root certificate of an external Certificate Authority and to create a server certificate.

You can also use Method 3 if your company or agency operates its own Certificate Authority. Use the APC Security Wizard in the same way, but use your own Certificate Authority in place of a commercial Certificate Authority.

Choosing a method for your system

Using the Secure Socket Layer (SSL) protocol, you can choose any of the following methods for using digital certificates.

Method 1: Use APC's default certificate. When you enable SSL, you must reboot the Management Card. During rebooting, if no server certificate exists on the Management Card, the Management Card generates a default server certificate that is signed by APC but that you cannot configure.

This method has the following advantages and disadvantages:

- **Advantages:**
  - Before they are transmitted, the user name and password for Management Card access and all data to and from the Management Card are encrypted.
  - You can use this default server certificate to provide encryption-based security while you are setting up either of the other two digital certificate options, or you can continue to use it for the benefits of encryption that SSL provides.
- **Disadvantages:**
  - The Management Card takes up to 5 minutes to create this certificate, and the Web interface is not available during that time. (This delay occurs the first time you log on after you enable SSL.)
  - This method does not include the browser-based authentication provided by a CA certificate (a certificate signed by a Certificate Authority) as Methods 2 and 3 provide. There is no CA Certificate cached in the browser. Therefore, whenever you log on to the Management Card, the browser generates a security alert,

indicating that a certificate signed by a trusted authority is not available and asking if you want to proceed.

– The default server certificate on the Management Card has the Management Card's serial number in place of a valid *common name* (the DNS name or the IP address of the Management Card). Therefore, although the Management Card can control access to its Web interface by user name, password, and account type (e.g., **Administrator**, **Device Manager**, or **Read Only User**), the browser cannot authenticate what Management Card is sending or receiving data.
– The length of the *public key* (RSA key) that is used for encryption when setting up an SSL session is only 768 bits. (The public key used in Methods 2 and 3 is 1024 bits, providing more complex encryption and consequently a higher level of security.)

Method 2: Use the APC Security Wizard to create a CA certificate and a server certificate. You use the APC Security Wizard to create two digital certificates:

- A *CA root certificate* (Certificate Authority root certificate) that the APC Security Wizard uses to sign all server certificates and which you then install into the certificate store (cache) of the browser of each user who needs access to the Management Card.
- A *server certificate* that you upload to the Management Card. When the APC Security Wizard creates a server certificate, it uses the CA root certificate to sign the server certificate.

The Web browser authenticates the Management Card sending or requesting data:

- To identify the Management Card, the browser uses the *common name* (IP address or DNS name of the Management Card) that was specified in the server certificate's *distinguished name* when the certificate was created.
- To confirm that the server certificate is signed by a "trusted" signing authority, the browser compares the signature of the server certificate with the signature in the root certificate cached in the browser. An expiration date confirms whether the server certificate is current.

This method has the following advantages and disadvantages.

- **Advantages:**
  - Before they are transmitted, the user name and password for Management Card access and all data to and from the Management Card are encrypted.
  - The length of the *public key* (RSA key) that is used for encryption when setting up an SSL session is 1024 bits, providing more complex encryption and consequently a higher level of security

than the public key used in Method 1. (This longer encryption key is also used in Method 3.)

  - The server certificate that you upload to the Management Card enables SSL to authenticate that data are being received from and sent to the correct Management Card. This provides an extra level of security beyond the encryption of the user name, password, and transmitted data.
  - The root certificate that you install to the browser enables the browser to authenticate the Management Card's server certificate to provide additional protection from unauthorized access.

- **Disadvantage:**

  Because the certificates do not have the digital signature of a commercial Certificate Authority, you must load a root certificate individually into the certificate store (cache) of each user's browser. (Browser manufacturers already provide root certificates for commercial Certificate Authorities in the certificate store within the browser. See Method 3.)

Method 3: Use the APC Security Wizard to create a certificate-signing request to be signed by the root certificate of an external Certificate Authority and to create a server certificate. You use the APC Security Wizard to create a request (a **.csr** file) to send to a Certificate Authority. The Certificate Authority returns a signed certificate (a **.crt** file) based on information you submitted in your request. You then use the APC Security Wizard to create a server certificate (a .**p15** file) that includes the signature from the root certificate returned by the Certificate Authority. You upload the server certificate to the Management Card.

You can also use Method 3 if your company or agency operates its own Certificate Authority, Use the APC Security Wizard in the same way, but use your own Certificate Authority in place of a commercial Certificate Authority.

This method has the following advantages and disadvantages.

- **Advantages:**
  - Before they are transmitted, the user name and password for Management Card access and all data to and from the Management Card are encrypted.
  - You have the benefit of authentication by a Certificate Authority that already has a signed root certificate in the certificate cache of the browser. (The CA certificates of commercial Certificate Authorities are distributed as part of the browser software, and a Certificate Authority of your own company or agency has probably already loaded its CA certificate to the browser store of each user's browser.) Therefore, you do not have to upload a root certificate to the browser of each user who needs access to the Management Card.
  - The length of the *public key* (RSA key) that is used for setting up an SSL session is 1024 bits, providing more complex encryption and consequently a higher level of security than the public key

used in Method 1 (This longer encryption key is also used in Method 2.)

  - The server certificate that you upload to the Management Card enables SSL to authenticate that data are being received from and sent to the correct Management Card. This provides an extra level of security beyond the encryption of the user name, password, and transmitted data.
  - The browser matches the digital signature on the server certificate that you uploaded to the Management Card with the signature on the CA root certificate that is already in the browser's certificate cache to provide additional protection from unauthorized access.

- **Disadvantages:**
  - Setup requires the extra step of requesting a signed root certificate from a Certificate Authority.
  - An external Certificate Authority may charge a fee for providing signed certificates.

Firewalls

Although some methods of authentication provide a higher level of security than others, complete protection from security breaches is almost impossible to achieve. Well-configured firewalls are an essential element in an overall security scheme.

Troubleshooting

Management Card

Management Card access problems

For problems that are not described here, see the troubleshooting flowcharts in *.\trouble* on the APC Network Management Card *utility* CD. If the problem still persists, see Warranty and Service.

Problem	Solution
Unable to ping the Management Card	If the Management Card's Status LED is green, try to ping another node on the same network segment as the Management Card. If that fails, it is not a problem with the Management Card. If the Status LED is not green, or if the ping test succeeds, perform the following checks: • Verify that the Management Card is properly seated in the UPS or expansion chassis • Verify all network connections • Verify the IP addresses of the Management Card and the NMS. • If the NMS is on a different physical network (or subnetwork) from the Management Card, verify the IP address of the default gateway (or router). • Verify the number of subnet bits for the Management Card's subnet mask.
The terminal program cannot allocate the communications port when you try to configure the Management Card	Before you can use a terminal to configure the Management Card, you must shut down any application, service, or program using the communications port.

Problem	Solution
Cannot access the Web interface	• Verify that HTTP or HTTPS access is enabled • Verify that you can ping the adapter • Verify that you are using a Web browser that is supported for the Network Management Card. See Supported Web browsers.)

SNMP issues

The following table describes known SNMP problems.

Problem	Solution
Unable to perform a GET	• Verify the read (GET) community name. • Use the control console or Web interface to ensure that the NMS has access. See SNMP.
Unable to perform a SET	• Verify the read/write (SET) community name. • Use the control console or Web interface to ensure that the NMS has write (SET) access. See SNMP.
Unable to receive traps at the NMS	Query the **mconfigTrapReceiverTable** PowerNet MIB OID to verify that the NMS IP address is listed correctly, and the community name defined for the NMS matches the community name in the table. If either is not correct, use SETs to the **mconfigTrapReceiverTable** OIDs, or use the control console or Web interface to correct the trap receiver definition. See SNMP.
Traps received at an NMS are not identified	See your NMS documentation to verify that the traps are properly integrated in the alarm/trap database.

Synchronization problems

Problem	Solution
A Synchronized Control Group member does not participate in a synchronized action.	Make sure the group member's status is set to **Enabled**. Also check the group member's battery capacity, if the synchronized action required UPSs to turn on.
An attempt to add a member to a Synchronized control group fails.	The **Multicast IP Address**, **Synchronized Control Group Number**, and firmware version must match those of other members of the group.

Product Information

Warranty and Service

Limited warranty

APC warrants the Network Management Card to be free from defects in materials and workmanship for a period of two years from the date of purchase. Its obligation under this warranty is limited to repairing or replacing, at its own sole option, any such defective products. This warranty does not apply to equipment that has been damaged by accident, negligence, or misapplication or has been altered or modified in any way. This warranty applies only to the original purchaser.

Warranty limitations

Except as provided herein, APC makes no warranties, express or implied, including warranties of merchantability and fitness for a particular purpose. Some jurisdictions do not permit limitation or exclusion of implied warranties; therefore, the aforesaid limitation(s) or exclusion(s) may not apply to the purchaser.

Except as provided above, in no event will APC be liable for direct, indirect, special, incidental, or consequential damages arising out of the use of this product, even if advised of the possibility of such damage.

Specifically, APC is not liable for any costs, such as lost profits or revenue, loss of equipment, loss of use of equipment, loss of software, loss of data, costs of substitutes, claims by third parties, or otherwise. This warranty gives you specific legal rights and you may also have other rights, which vary according to jurisdiction.

Obtaining service

To obtain support for problems with your Network Management Card:

1. Note the serial number and date of purchase. The serial number is on the Management Card itself and on the Quality Assurance slip shipped with the card.
2. Contact Customer Support at a phone number listed under APC Worldwid Customer Support at the end of this manual. A technician will try to help you solve the problem by phone.
3. If you must return the product, the technician will give you a return material authorization (RMA) number. If the warranty expired, you will be charged for repair or replacement.
4. Pack the unit carefully. The warranty does not cover damage sustained in transit. Enclose a letter with your name, address, RMA number and daytime phone number; a copy of the sales receipt; and a check as payment, if applicable.
5. Mark the RMA number clearly on the outside of the shipping carton.
6. Ship by insured, prepaid carrier to the address provided by the Customer Support technician.

The Network Management Card is sensitive to static electricity. When handling the Management Card, touch only the end plate while using one or more of these electrostatic-discharge devices (ESDs): wrist straps, heel straps, toe straps, or conductive shoes.

Recycling the Battery

The Network Management Card contains a removable, lithium coin-cell battery. When discarding this battery, you must follow local rules for recycling.

Life-Support Policy

General policy

American Power Conversion (APC) does not recommend the use of any of its products in the following situations:

- In life-support applications where failure or malfunction of the APC product can be reasonably expected to cause failure of the life-support device or to affect significantly its safety or effectiveness.
- In direct patient care.

APC will not knowingly sell its products for use in such applications unless it receives in writing assurances satisfactory to APC that (a) the risks of injury or damage have been minimized, (b) the customer assumes all such risks, and (c) the liability of American Power Conversion is adequately protected under the circumstances.

Examples of life-support devices

The term *life-support device* includes but is not limited to neonatal oxygen analyzers, nerve stimulators (whether used for anesthesia, pain relief, or other purposes), autotransfusion devices, blood pumps, defibrillators, arrhythmia detectors and alarms, pacemakers, hemodialysis systems, peritoneal dialysis systems, neonatal ventilator incubators, ventilators (for adults and infants), anesthesia ventilators, infusion pumps, and any other devices designated as “critical” by the U.S. FDA.

Hospital-grade wiring devices and leakage current protection may be ordered as options on many APC UPS systems. APC does not claim that units with these modifications are certified or listed as hospital-grade by APC or any other organization. Therefore these units do not meet the requirements for use in direct patient care.

Specifications

Electrical

Item	Specification
Acceptable input voltage	19-30 VDC
Maximum total current draw	110 mA

Physical

Item	Specification
Size (H × W × D)	1.46 ×4.75 ×4.3 in (3.7 ×12.1 ×10.9 cm)
Weight	.25 lb (.11 kg)
Shipping weight	.8 lb (.36 kg)

Index

A

About System 33
Access
  FTP Server 41
  limiting NMS SNMP access by IP address 49
  security options for each interface 143
  troubleshooting 163
Access Type setting 49
Actions 121
Actual Battery Bus Voltage 78
Actual Battery Voltage 78
Add Client IP 98
Advanced settings
  Client ID 39, 137
  Domain Name 39, 137
  Host Name 39, 137
  On Retry Failure 39
  Port Speed 39, 137
  Retry Then Fail 39
  TCP/IP settings 39
  User Class 39, 137
  Vendor Class 39, 137
Alarm if Load Over 91
Alarm if Redundancy Under 91
Alarm if Runtime Under 91
Analog modem
  AP9618 feature 1
  configuring control console dial-in 69
  connector on AP9618 faceplate 6
  modem connector 8
  using for control console access 13
AP9618U upgrade kit 2
AP9619U upgrade kit 2
APC OS 33
Apparent Load Power 76
Apply Local Computer Time 66
Audible Alarm 94
Authentication
  MD5 147
  Phrase 64
  SNMP Traps 125
  User Manager setting in the control console 64
  with SSL 152
Auto Logout 64

B

Battery Capacity 78
Battery Current 78
Battery status
  Actual Battery Bus Voltage 78
  Actual Battery Voltage 78
  Battery Capacity 78
  Battery Current 78
  Battery Voltage 78
  Calibration Date 78
  Calibration Result 78
  Nominal Battery Voltage 78
  Number of Bad Batteries 78
  Number of External Batteries 78
  Runtime Remaining 78
  Self-Test Date 78
  Self-Test Result 78
Battery Voltage 78
Boot mode 134
Boot mode settings
  BOOTP & DHCP 38
  BOOTP only 38
  DHCP only 38
  Manual 38

BOOTP
After IP Assignment setting 138
Boot mode settings 38
BOOTP Only boot mode setting 38
Communication
Client ID 39
User Class 39
Vendor Class 39
DHCP & BOOTP boot process 135
Remain in DHCP & BOOTP mode setting 138
Status LED indication for making BOOTP requests 9
BOOTP & DHCP boot mode setting 38
Browsers
CA certificates in browser's store (cache) 152
supported for Management Card 23
Bypass Input Voltage 74
Bypass Lower Voltage 90
Bypass Upper Voltage 90

C

Calibration
Date 78
Result 78
Certificates
choosing which method to use 154
creating and installing for SSL 154
methods
APC Security Wizard creates all certificates 157
Use a Certificate Authority (CA) 159
Use APC's default certificate 155
CipherSuite
Choosing SSL encryption ciphers and hash algorithms 57
purpose of the algorithms and ciphers 153
Client ID setting 39, 137
Community Name 125
SNMP 49
verifying correctness 164
Configuration menu
Battery 92
General Settings 94
option in UPS menu 89
Shutdown Parameters 92
Configure Synchronized Control 107
Configured Client IP Addresses 98
Configuring
MD5 authentication 148
proxy server not to proxy the Management Card 23
SSH 42
SSL/TLS 54
Contact identification (whom to contact) 65
Contact settings (environmental) 112
Contact status (environmental) 111
Control console
Device Manager menu 21
External and Internal Environmental Monitor Settings options 109
main screen 16
navigating menus 20
refreshing menus 20
Control menu
Put UPS In Bypass 87
Put UPS To Sleep 87
Put UPS To Sleep Gracefully 87
Reboot UPS 86
Reboot UPS Gracefully 86
Self-Test (control console) 80
Simulate Power Failure (control console) 80
Start/Stop Runtime Calibration (control console) 80
Take UPS Off Bypass 87
Test UPS Alarm (control console) 80
Turn UPS Off 85
Turn UPS Off Gracefully 85
Turn UPS On 85

D

Data log
configuration 133
importing into spreadsheet 118
Log Interval setting 133
using FTP or SCP to retrieve 118
Date & Time settings 66
Apply Local Computer Time 66
GMT Offset (TIme Zone) 66
Manual 66
Network Time Protocol (NTP) 66
Primary NTP Server 66
Secondary NTP Server 66
Set Manually 66
Synchronize with NTP Server 66
Update Interval 66
Delete SSH Host Keys and SSL Certificates 67
Detailed Status option 73
Detailed UPS Information option 73
Device Manager menu 71
control console 21
Utility Power Status 74
DHCP
After IP Assignment setting 138
APC cookie 139
as feature of Network Management Cards 1
Boot mode settings 38
Communication
Client ID 39
User Class 39
Vendor Class 39
Configuration 134
Cookie Is setting 138
DHCP & BOOTP boot process 135
DHCP Only boot mode setting 38
Management Card settings 135
Remain in DHCP & BOOTP mode setting 138
Require vendor specific cookie to accept DHCP Address setting 138
response options 139
Retry Then Stop setting 138
Status LED indication for making DHCP requests 9
Diagnostics menu
Self-Test 80
Simulate Power Failure 80
Start/Stop Runtime Calibration 80
Test UPS Alarm 80
Disabling
e-mail to a recipient 129
event logging 122
sending any traps to an NMS 125
sending authentication traps to an NMS 125
synchronized group membership 107
use of a proxy server 23
Domain Name setting 39, 137

E

Electrical specifications 169
E-mail
configuring 126
Email action 123
Email option, Events menu 128
Email Recipients
Format 130
Generation 129
Local SMTP Server 129
menu option 128
To Address 129
Use SMTP Server 129
enabled by default for severe events 123
enabling and disabling 129
message format (long or short) 130
reason to use local DNS server 127
setting up an account for the Management Card 129
using for paging 129

Enabling
e-mail forwarding to external SMTP servers 129
e-mail to a recipient 129
MD5 authentication 147
sending any traps to an NMS 125
sending authentication traps to an NMS 125
SSH 44
Synchronized Group Membership 107
Telnet 44
Encryption
with SSH and SCP 150
with SSL 54
Environment menu
Threshold and Contact Details 110
Environmental monitor
contact settings 112
contact status 111
control console status report 16, 18, 110
Device Manager options in control console 21
management through the Web interface 23
probe settings 112
probe status 111
Settings options in the control console 109
status icons in the Web interface 30
Web interface status report 27, 28, 110
Error messages 26
Event log 122
accessing 20
deleting by typing d in control console 118
disabling 122
using Ctrl-L to display the log in control console 118
using FTP del command 120
using FTP or SCP to retrieve 118
event.txt file
contents 118
importing into spreadsheet 118
Events menu
Actions 121
Email (Web interface) 123
Email Recipients (Web interface) 128
Event log 122
Log option 117
SNMP traps 123
Syslog action 123
External Batteries 94

F

Facility setting 51
Fault Tolerance
Present kVA Capacity 77
Redundancy 77
Faults & Alarms 73
Fingerprints, displaying and comparing 43
Firewall, as essential to security 161
Firmware
versions displayed on main screen 17
From Address 127
FTP 41
disabling when SCP is used 41
using to retrieve text version of event or data log 118

G

General Settings 94
Audible Alarm 94
External Batteries 94
Last Battery Replacement 94
Self-Test Schedule 94
Simple Signal Shutdowns 94
UPS Name 94
Generation setting, Email Recipients 129
GET commands, troubleshooting 164
GMT Offset (TIme Zone) 66

H

Help
About System option (Web interface) 33
on control console 20
High Transfer Voltage 90
Host key
file name 47
file status 47
fingerprints
displaying for versions 1 and 2 48
generated by the Management Card 43
transferring to the Management Card 43, 47
Host Name setting 39, 137
HTTP Port 56
HTTP protocol mode 55
HTTPS Port 56
HTTPS protocol mode 55
Hyperlinks, defining 68

I

Identification 65
displaying on main screen 17
MIB-II variables 65
If UPS Fails (Utility Line setting) 91
Input Current 74
Input Frequency 74
Input Voltage 74
Integrated Environmental Monitor
AP9618 and AP9619 feature 4, 6, 8
output relay connection pins 8
output relay settings 113
output relay status 111
zone 1 and 2 (input contact) connector pins 8
IP addresses
for Configure Multiple/Parallel UPS IP Address 95
for PowerChute Network Shutdown clients 98
of DNS server for e-mail 126
of trap receivers 125
to limit access to specified NMSs 49

L

Last Battery Replacement 94
Life support 168
Links, redirecting 34, 68
Load Current 76
Load Power 76
Local SMTP Server 129
Location 65
Lock icon indicating SSL is enabled. 55
Logging on
DNS name or IP address matched to common name 25
error messages for Web interface 26
Web interface 25
Login date and time
control console 17
Web interface 28
Low Transfer Voltage 90
Low-Battery Duration 92

M

Main screen
displaying identification 17
firmware values displayed 17
login date and time 17
status 18
Up Time 17
user access identification 17

Management Card
port assignment 145
Manual boot mode setting 38
Manual option to set date and time 66
Maximum Line Voltage 74
Maximum Shutdown Time
PowerChute Network Shutdown 98, 99
Shutdown Parameters 92
Maximum-Shutdown-Time
negotiation 99, 100
MD5
browser settings required 23
enabling 147
how it performs authentication 148
requirement of login credentials to access cached Web page 153
Menus
Configuration 89, 92
Control Console 19
Data 32, 132
Device Manager 71
Environment 32, 110
event-related 32
Events 32, 114
Help 33
Links 34, 68
Network 32, 35
System 33, 61
UPS 32, 71, 89
MIB-II Identification variables 65
Minimum Line Voltage 74
Module Diagnostics & Information 96
Module Status 96
Monitor Name 95
Multicast IP Address parameter 108

N

Name of Scheduled Shutdown 103
Network Management Card,
See Management Card
Network menu
Email (control console) 128
FTP Server 41
Telnet/SSH 42
Web/SSL/TLS 54
Network Time Protocol (NTP) 66
NMS IP setting 49
NMS receiving unidentified trap, troubleshooting 164
Nominal Battery Voltage 78
NTP 66
Number of Bad Batteries 78
Number of External Batteries 78

O

On Retry Failure setting 39
Operating Frequency field (control console) 74, 76
OS, APC 33
Output Current 76
Output Frequency 76
Output Frequency Range 90, 91
Output kVA 76
Output Power 76
Output Power Percentage 76
Output Power Status
Apparent Load Power 76
Load Current 76
Load Power 76
Output Current 76
Output Frequency 76
Output kVA 76
Output Power 76
Output Power Percentage 76
Output VA at n+0 76
Output VA at n+1 76
Output Voltage 76
Output Watts at n+0 76
Output Watts at n+1 76
Peak Output Current 76
UPS menu option 75

Output relay
AP9618 and AP9619 feature 1, 6, 8
control console status report 16, 18, 111
settings 113
Web interface status report 27, 28, 111
Output VA at n+0 76
Output VA at n+1 76
Output Voltage 76, 90, 91
Output Watts at n+0 76
Output Watts at n+1 76

P

Paging by using e-mail 129
Password change for security 145
Passwords
default for Administrator, Device Manager, and Read Only User 25
for NMS that is a trap receiver 125
User Manager access 64
using non-standards ports as extra passwords 145
Peak Output Current 76
Physical specifications 169
Ping utility
for troubleshooting Management Card access 162
for troubleshooting Management Card network connection 41
Port Speed setting 39, 137
Ports
assigning 145
default
for FTP Server 41
for HTTP 56
for HTTPS 56
for SSH 45
for Telnet 45
using a non-default port
for FTP 41
for HTTP 56
for HTTPS 56
for SSH 45
for Telnet 45
Power Synchronized Delay 83
PowerChute Network Shutdown
Add Client IP 98
Configured Client IP Addresses 98
Maximum Shutdown Time 98, 99
Shutdown Behavior 98
Present kVA Capacity 77
Primary NTP Server 66
Probe settings 112
Probe status 111
Protocol Mode
selecting for control console access 44
selecting for Web access 55
Proxy servers
configuring not to proxy the Management Card 23
disabling use of 23
Put UPS
To Sleep 87
To Sleep Gracefully 87
Put UPS In Bypass 87

R

Read access by an NMS 49
Reboot
UPS 86
UPS Gracefully 86
Reboot Card 67
Receiver NMS IP 125
Recipient's SMTP Server 129
Redundancy 77

Reset Card to Defaults 67
Reset Card to Defaults Except TCP/IP 67
Reset Only TCP/IP to Defaults 67
Restart Network Management Card
  preventing restart for inactivity 12
Retry Then Fail setting 39
Retry Then Stop setting (DHCP) 138
Return Battery Capacity 92
Return Delay 93
RSA key exchange algorithm 57
Runtime Remaining 78

S

Scheduling
  UPS self-tests 81
  UPS shutdowns 101
Scheduling shutdownsof UPSs in a Synchronized Control Group 104
SCP
  enabled and configured with SSH 42, 151
  using to retrieve text version of event or data log 118
Secondary NTP Server 66
Secure CoPy. *See* SCP.
Secure Hash Algorithm (SHA) 57
Secure SHell. *See* SSH.
Secure Socket Layer
  See SSL.
Security
  authentication
    authentication vs. encryption 147
    through digital certificates with SSL 152
    with MD5 148
  certificate-signing requests 152
  disabling less secure interfaces 148, 151
  encryption with SSH and SCP 150
  immediately changing username and password 145
  options for each interface 143
  planning and implementing 143, 147
  SCP as alternative to FTP 151
  SSL
    choosing a method to use certificates 154
    CipherSuite algorithms and ciphers 153
  supported SSH clients 42
  using MD5 authentication 148
  using non-standards ports as extra passwords 145
Self-Test Date 78
Self-Test Result 78
Self-Test Schedule 94
Self-Test, Diagnostics menu option 80
Send DNS Query 40
Sensitivity 90
SET commands, troubleshooting 164
Set Manually, date and time 66
Severity levels (of Events)
  Informational 122
  None 122
  Severe 122
  Warning 122
Shutdown Behavior 98
Shutdown Delay 92
Shutdown Parameters 92
  Low-Battery Duration 92
  Maximum Shutdown Time 92
  Return Battery Capacity 92
  Return Delay 93
  Shutdown Delay 92
  Sleep Time 93
Shutdowns
  How to edit, disable, or delete 105
  how to schedule 101
  how to schedule synchronized 104
Signal servers 85
Simple Signal Shutdowns 94
Simulate Power Failure 80

Sleep Time 93
SMTP
From Address 127
SMTP Server 127
SNMP
Access Type setting 49
Authentication Traps 125
Community Name setting 49
enabling and disabling 49
NMS IP setting 49
SNMP traps option 123
troubleshooting problems 164
Specifications 169
electrical 169
physical 169
SSH
configuring 42
enabling 42
encryption 150
fingerprints,displaying and comparing 43
host key
as identifier that cannot be falsified 150
file name 47
file status 47
transferring to the Management Card 43
modifying the Port setting 45, 56
obtaining an SSH client 42
server configuration 46
v1 Encryption Algorithms 46
v2 Encryption Algorithms 46
SSL
authentication throughdigital certificates 152
certificate signing requests 152
encryption ciphers and hash algorithms 57
Start/Stop Runtime Calibration 80
Status
in detail 73
in Web interface 28
on control console main screen 18
summary 27, 73
UPS menu option 73
Status icons in the Web interface 29
Sync Control
Configure Synchronized Control 107
Synch Control Group Status 106
Synchronize with NTP Server 66
Synchronized actions
LED behavior during 83
Put UPS to Sleep 87
Put UPS to Sleep Gracefully 87
Reboot UPS 86
Reboot UPS Gracefully 86
Turn UPS off 85
Turn UPS Off Gracefully 85
Turn UPS Off with shutdown delay. 83
Synchronized Control Groups
configurable parameters 107
initiatiating a synchronized action. 82
Power Synchronized Delay 83
the synchronization process 83
Syslog
enabled by default for all events 123
Events menu option 123
Facility setting 51
System
information, obtaining 33
Name 65
System menu 61
About System option (control console) 33
Date & Time 66
Identification 65
Tools 67
User Manager 63
System: Coldstart event 99
System: Warmstart event 99

T

Take UPS off Bypass 87
TCP/IP
  Advanced settings 39
  Boot mode 38
  Client ID setting 39, 137
  Current settings fields 37
  default gateway 37, 38
  defining settings for the Management Card 37
  Domain Name setting 39, 137
  Host Name setting 39, 137
  On Retry Failure setting 39
  Port Speed setting 39, 137
  restoring default settings 67
  Retry Then Fail setting 39
  setting port assignments for extra security 145
  subnet mask 37, 38
  system IP address 37, 38
  User Class setting 39, 137
  Vendor Class setting 39, 137
Telnet/SSH
  Access option 44
  host key fingerprints
    displaying 48
  modifying the Port settings 45
  option in Network menu 42
  selecting the protocol mode 44
  SSH host key file name 47
  SSH host key file status 47
  SSH Port option 45
  SSHv1 Encryption Algorithms 46
  SSHv2 Encryption Algorithms 46
  Telnet Port option 45
Test UPS Alarm 80
Testing the network connection to the DNS server 40
Threshold and Contact Details 110
Time Zone 66
To Address 129
Tools menu 67
  Delete SSH Host Keys and SSL Certificates 67
  Reboot Card 67
  Reset Card to Defaults 67
  Reset Card to Defaults Except TCP/IP 67
  Reset only TCP/IP to Defaults 67
  XMODEM 67
Transport Layer Security (TLS) 152
Trap Generation 125
Trap Receivers
  Authentication Traps 125
  Community Name 125
  Receiver NMS IP 125
  Trap Generation 125
Traps
  troubleshooting inability to receive traps 164
  troubleshooting unidentified traps 164
Troubleshooting
  by pinging a network node 162
  communications port allocation 162
  e-mail configuration 127
  GET and SET performance 164
  inability to access Web interface 163
  inability to perform GETs 164
  inability to perform SETs 164
  inability to receive traps 164
  problems logging on to Web interface 25
  proxy server problems 23
  SNMP problems 164
  Traps, not identified 164
  using flowcharts on the utility CD-ROM 162
  verification checklist 162
Turn UPS Off 85
Turn UPS Off Gracefully 85
Turn UPS On 85

U

Unidentified traps, troubleshooting 164
Up Time
  control console main screen 17
  Web interface 28
Update Interval 66
Upgrade kits, to add modem and environmental monitor 2
UPS menu 71
  Configuration 89
  Detailed Status 73
  Detailed UPS Information 73
  Faults & Alarms 73
  Module Diagnostics & Information 96
  Module Status 96
  Output Power Status 75
  Scheduled Tests 81
  Status 73
UPS Name 94
UPS status icons in the Web interface 29
URL address formats 26
Use SMTP Server 129
User access identification, control console interface 17
User Class setting 39, 137
User Manager 63
  Authentication 64
  Authentication Phrase 64
  Auto Logout 64
  Password 64
  User Name 64
User Name
  change immediately for security 145
  default for Administrator, Device Manager, and Read Only User 25
  User Manager access 64
Utility Line Settings
  Bypass Lower Voltage 90
  Bypass Upper Voltage 90
  High Transfer Voltage 90
  If UPS Fails 91
  Low Transfer Voltage 90
  Output Frequency 90, 91
  Output Voltage 90, 91
  Sensitivity 90
  Vout Reporting 90, 91
Utility Power Status 74
Utility Voltage Status
  Bypass Input Voltage 74
  Input Current 74
  Input Frequency 74
  Input Voltage 74
  Maximum Line Voltage 74
  Minimum Line Voltage 74

V

Vendor Class setting 39, 137
View the refreshing status page hyperlink 72, 95
Vout Reporting 90, 91

W

Web browsers supported 23
Web interface 23
  enable or disable protocols 55
  logging on 25
  logon error messages 26
  Modifying the Port setting
    for FTP 41
    for HTTP 56
    for HTTPS 56
    for SSH 45
    for Telnet 45

status 28
summary page 27
troubleshooting access problems 163
Up Time 28
URL address formats 26

X

XMODEM 67

APC Worldwide Customer Support

Customer support for this or any other APC product is available at no charge in any of the following ways:

- Visit the APC Web site to find answers to frequently asked questions (FAQs), to access documents in the APC Knowledge Base, and to submit customer support requests.
  - **www.apc.com** (Corporate Headquarters)

    Connect to localized APC Web sites for specific countries, each of which provides customer support information.
  - **www.apc.com/support/**

    Global support with FAQs, knowledge base, and e-support.
- Contact an APC Customer Support center by telephone or e-mail.
  - Regional centers:

APC headquarters U.S., Canada	(1)(800)800-4272 (toll free)
Latin America	(1)(401)789-5735 (USA)
Europe, Middle East, Africa	(353)(91)702020 (Ireland)
Japan	(0) 35434-2021

  - Local, country-specific centers: go to **www.apc.com/support/contact** for contact information.

Contact the APC representative or other distributor from whom you purchased your APC product for information on how to obtain local customer support.

Copyright

Cryptlib, the toolkit used to develop the library of cryptographic routines in the Network Management Card: copyright © 1998 Digital Data Security, Ltd., New Zealand.

The Network Management Card is certified for use with APC InfraStruXure™ systems.

990-0385C **06/2003**